UNIVERSITÀ DEGLI STUDI DEL SANNIO

DIPARTIMENTO DI INGEGNERIA
CORSO DI LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

Automated Analysis of Emerging Ransomware Strategies

Project Report Sicurezza delle Reti e dei Sistemi Software 2024/2025

Studenti:
Rita Lamparelli 399000607
Lucy Masella 399000586
Marco Rossi 399000605

Docente:
Corrado Aaron Visaggio
Referente:
Pietro Melillo

Introduzione

Negli ultimi anni, gli attacchi ransomware sono diventati una delle minacce più pervasive e distruttive nel panorama della sicurezza informatica. Questi attacchi consistono nella crittografia dei dati di un'organizzazione o individuo, accompagnata da una richiesta di riscatto in cambio del ripristino dell'accesso. L'obiettivo del presente progetto è analizzare in modo sistematico e quantitativo i dati relativi agli attacchi ransomware, al fine di individuare pattern significativi, settori economici e aree geografiche maggiormente vulnerabili, nonché tendenze temporali e comportamenti specifici dei gruppi criminali. In letteratura, è riconosciuta la necessità di sviluppare e perfezionare approcci automatizzati per la detection di attacchi ransomware. L'evoluzione rapida e l'adattabilità di questi attacchi rendono particolarmente ardua la creazione di sistemi di rilevamento efficaci. Attraverso lo studio approfondito dei dati e delle dinamiche degli attacchi, questo progetto potrebbe contribuire all'identificazione di strategie di attacco comuni, che, se comprese, potrebbero essere utilizzate per affinare gli strumenti di rilevamento automatico e per prevenire futuri attacchi.

Questa analisi si propone di fornire una panoramica dettagliata su:

- La distribuzione geografica delle vittime.
- I settori economici più colpiti.
- I gruppi ransomware più attivi e le loro strategie.
- L'evoluzione temporale degli attacchi.
- L'influenza di fattori geopolitici sugli attacchi.

Descrizione del Dataset

Il dataset utilizzato per questa analisi rappresenta una raccolta di informazioni dettagliate sugli attacchi ransomware con doppia estorsione registrati negli ultimi anni. Ogni riga del dataset rappresenta un singolo attacco e contiene informazioni su vittime, gruppi ransomware e dettagli operativi. Di seguito, una descrizione delle principali colonne:

- **Victim**: Nome della vittima dell'attacco ransomware, che può corrispondere a un'azienda, un'organizzazione o un ente governativo.
- **Gang**: Nome del gruppo ransomware che ha effettuato l'attacco. Questa informazione permette di analizzare le strategie e i target principali di ciascun gruppo.
- **Date**: Data esatta in cui l'attacco è stato registrato. È utilizzata per analizzare tendenze temporali e identificare eventuali picchi o stagionalità negli attacchi.
- **Victim Country**: Paese in cui si trova la vittima dell'attacco, utile per analizzare la distribuzione geografica delle vittime.
- **Victim Sector**: Settore economico a cui appartiene la vittima (es. sanità, tecnologie, retail). Questo dato consente di identificare i settori maggiormente vulnerabili.
- **Number of Employees**: Numero di dipendenti dell'organizzazione colpita, suddiviso in intervalli. Fornisce indicazioni sulla dimensione delle organizzazioni bersagliate.
- **Sales:** Fatturato stimato dell'organizzazione, anch'esso suddiviso in intervalli. Utile per capire se i gruppi ransomware mirano principalmente a aziende di una certa fascia economica.

Stato dell’Arte

L'analisi dei ransomware ha assunto un'importanza centrale nell'ambito della cybersecurity, poiché questi attacchi continuano a evolversi, aumentando in frequenza e sofisticazione. In particolare, negli ultimi anni sono stati condotti diversi studi significativi che hanno approfondito le caratteristiche degli attacchi ransomware, le contromisure disponibili e le limitazioni esistenti nelle tecniche di difesa.

Uno di questi studi, "**Differential Area Analysis for Ransomware: Attacks, Countermeasures, and Limitations**", esamina la tecnica della Differential Area Analysis (DAA), che analizza le intestazioni dei file per distinguere tra file compressi, file regolarmente criptati e file criptati da ransomware. L'articolo esplora tre diversi tipi di attacco progettati per eludere il rilevamento tramite DAA, evidenziando le limitazioni di questa tecnica e proponendo nuove metodologie per potenziarne l'efficacia.

Un altro studio rilevante, **"Unveiling Dynamics and Patterns: A Comprehensive Analysis of Spreading Patterns and Similarities in Low-Labelled Ransomware Families"**, si propone di analizzare i grafi delle transazioni Bitcoin generati dai pagamenti ransomware. Gli obiettivi sono identificare i modelli di diffusione dei pagamenti per valutare l'evoluzione delle famiglie di ransomware e rilevare somiglianze tra varianti diverse che potrebbero essere potenzialmente controllate dallo stesso aggressore.

Inoltre, lo studio "**Understanding Crypto-Ransomware**" esamina l'evoluzione degli attacchi ransomware nell'ultimo decennio, mettendo in luce l'aumento della complessità degli attacchi, l'adozione di nuovi vettori di infezione e l'uso di algoritmi di crittografia avanzati. Gli autori analizzano circa 30 varianti di ransomware, rivelando un costante miglioramento nell'efficacia di queste minacce nel tempo.

A differenza degli studi precedenti, questa analisi adotta una prospettiva diversa, focalizzandosi sull'individuazione dei pattern d'attacco dei gruppi ransomware. A questo scopo, vengono esaminate le vittime colpite, identificando le caratteristiche che le accomunano, nonché eventuali relazioni tra il panorama politico e gli attacchi informatici. In particolare, si analizzano i fattori che potrebbero influenzare la scelta delle vittime da parte degli attaccanti, come la posizione geografica, le tensioni politiche o le vulnerabilità specifiche dei settori colpiti, offrendo così una visione più ampia delle dinamiche degli attacchi ransomware.

Questo approccio non è stato ampiamente trattato in ambito accademico, poiché la maggior parte degli studi tende a focalizzarsi maggiormente sull’analisi del comportamento del ransomware stesso, piuttosto che sull’identificazione di pattern di attacco comuni attraverso lo studio delle vittime. Tuttavia, alcune aziende e organizzazioni hanno adottato un tipo di analisi simile per comprendere meglio le dinamiche degli attacchi ransomware.

- La **Clusit** (Associazione Italiana per la Sicurezza Informatica) pubblica annualmente un rapporto che analizza in dettaglio gli incidenti informatici globali, con particolare attenzione agli attacchi ransomware. Questo rapporto fornisce una panoramica completa sui settori, le aziende e le regioni geografiche maggiormente colpiti, contribuendo così a tracciare i pattern e le tendenze emergenti nel panorama delle minacce informatiche.

- La **Semperis** ha condotto uno studio approfondito sull’evoluzione dei ransomware, con un focus su come le organizzazioni affrontano gli attacchi ripetuti e sull'importanza della resilienza digitale. Lo studio ha esaminato le motivazioni e le strategie dietro gli attacchi ransomware ricorrenti, offrendo una visione sulle tattiche utilizzate dai gruppi di attaccanti e le misure che le aziende devono adottare per proteggersi da minacce persistenti e sempre più sofisticate.

Analisi effettuate

Prima di procedere con le analisi, è stato effettuato un lavoro di normalizzazione del dataset tramite le seguenti operazioni:

- Correzione manuale degli errori grammaticali nei “Victim Sector” (es. *Agricolture* → *Agriculture*).
- Uniformazione dell’uso delle lettere maiuscole nei “Victim Sector” e nelle “Victim Country” (es. *italy* → *Italy*).
- Traduzione in lingua inglese delle “Victim Country” (es. *Ucraina* → *Ukraine*).
- Uniformazione dell’uso del singolare/plurale nei “Victim Sector” (es. *Technologies* → *Technology*).
- Rimozione di valori malformattati nelle colonne “Number of Employees” e “Sales” (es. *<2N/A56* → *null*).
- Rimozione delle vittime censurate dalla colonna “Victim” (es. *A*** → *null*).

Inoltre, per ciascuna domanda, non sono stati considerati gli attacchi con valori nulli nelle colonne di interesse per la specifica analisi.

1. Distribuzione geografica

1.1: Quali paesi registrano il maggior numero di vittime?

Sono state analizzate le colonne "Victim" e "Victim Country" del dataset, che contengono informazioni dettagliate sulle vittime degli attacchi ransomware e sul paese in cui sono localizzate. Per ottenere una panoramica più chiara, gli attacchi sono stati raggruppati per vittima, successivamente è stato effettuato un conteggio delle occorrenze per ciascun paese, in modo da evidenziare la distribuzione geografica degli attacchi. Una volta ottenuti i conteggi, sono state calcolate le percentuali di vittime per ogni paese per poi essere rappresentate in un grafico a torta (*Figura 1.1*). Per una migliore leggibilità e comprensione del grafico, i paesi che hanno subito meno del 2% degli attacchi totali sono stati raggruppati nella categoria "Other". Questo approccio consente di ridurre il numero di segmenti nel grafico, concentrandosi sui paesi con una maggiore concentrazione di vittime e facilitando l'analisi visiva della distribuzione geografica.

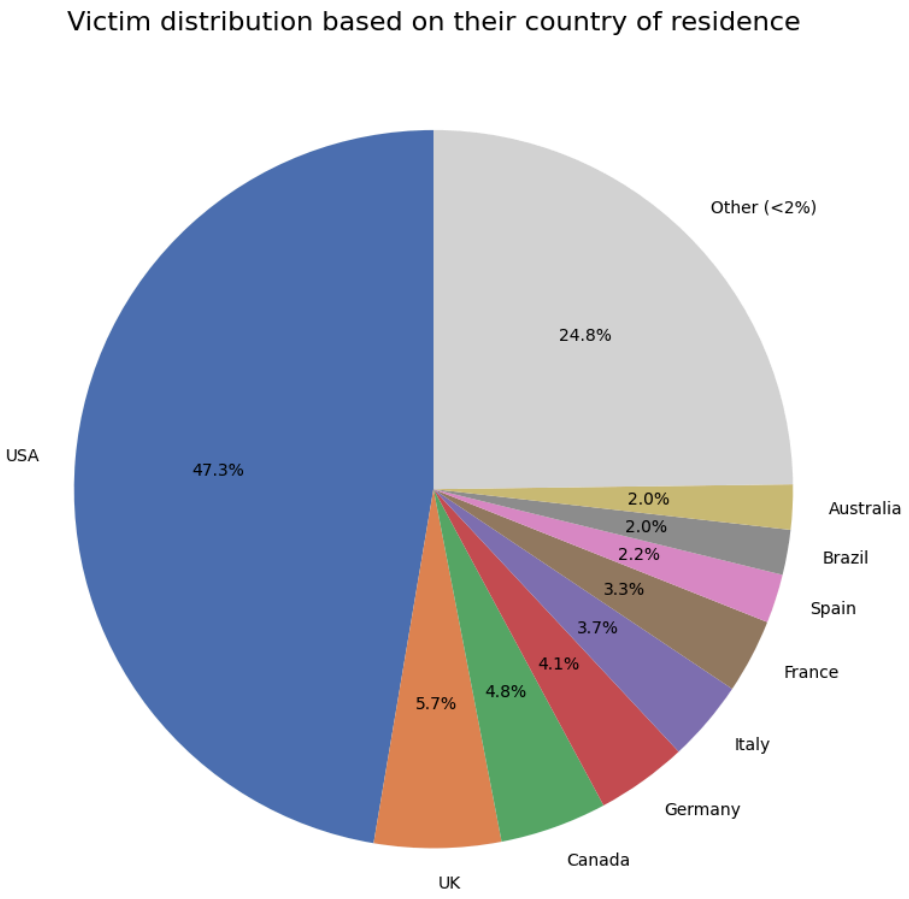

Figura 1.1: Distribuzione delle vittime in base al loro paese di appartenenza.

Si osserva una distribuzione fortemente sbilanciata: in effetti, il **75%** delle vittime totali è concentrato in soli **9 paesi** su un totale di 176 nazioni prese in considerazione. È evidente una centralizzazione degli attacchi, con alcune regioni geografiche che sono maggiormente colpite rispetto ad altre.

In particolare, gli **Stati Uniti** emergono come il paese più colpito, rappresentando da solo **quasi la metà** delle vittime totali. Questo potrebbe riflettere una serie di fattori, tra cui la dimensione economica e la presenza di molte organizzazioni vulnerabili nel paese, ma anche la sua centralità nel

panorama digitale globale, che lo rende un obiettivo privilegiato per i gruppi ransomware. È interessante notare come, sebbene la tecnologia e la sicurezza informatica negli Stati Uniti siano generalmente avanzate, l'ampiezza e la diversità delle organizzazioni presenti possano anche generare opportunità per gli attaccanti.

Per approfondire l'analisi, gli attacchi sono stati divisi per anno e rappresentati in diversi grafici a torta, uno per ciascun anno (*Figura 1.2*). Non sono emerse differenze significative rispetto alla distribuzione generale.

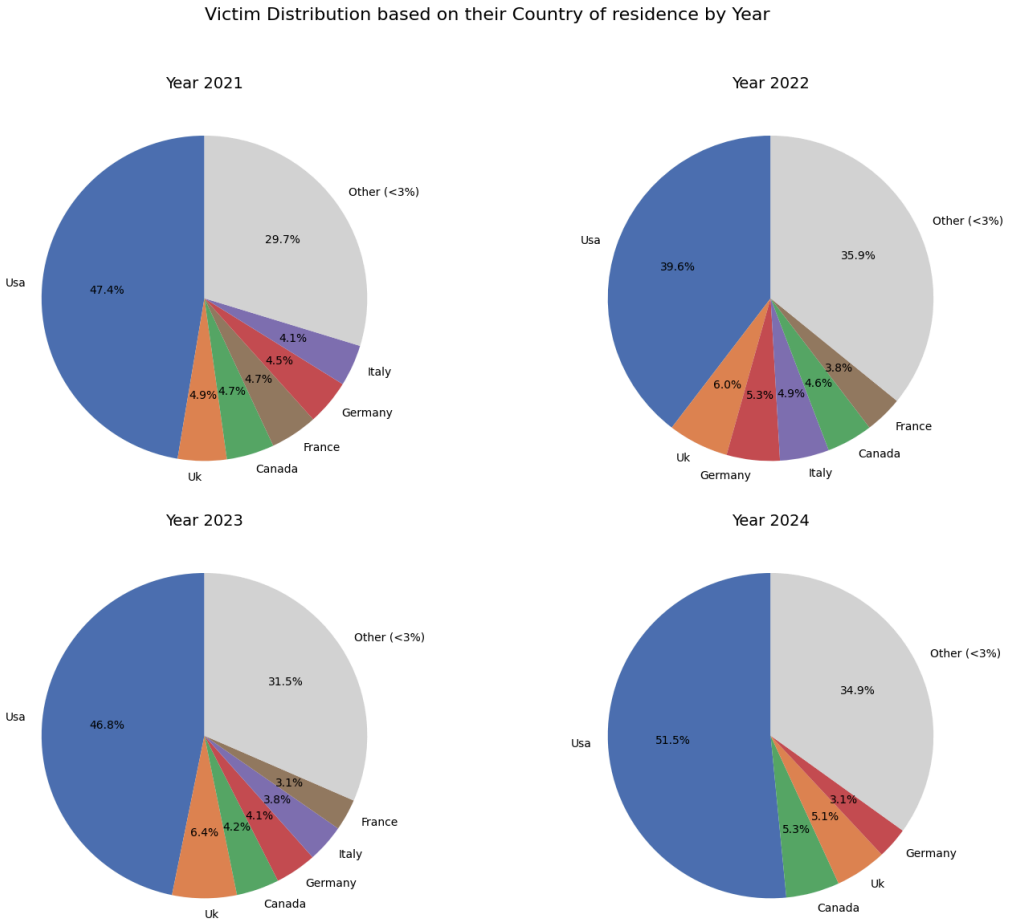

Figura 1.2: Distribuzione annuale delle vittime in base al loro paese di residenza.

1.2: Alcuni gruppi ransomware preferiscono colpire in determinati continenti o aree geografiche. Quali?

Sono state analizzate le colonne "Gang" e "Victim Country" del dataset per identificare i gruppi ransomware che concentrano una percentuale significativa dei loro attacchi in una singola nazione. L'analisi ha preso in considerazione esclusivamente i gruppi che hanno registrato più di 10 attacchi totali, di cui almeno il **50% indirizzati verso un singolo paese**. Questo approccio ha permesso di evidenziare pattern geografici specifici legati alle strategie operative di tali gruppi.

Tuttavia, considerando l'elevata concentrazione di attacchi negli Stati Uniti, che già emerge come una nazione particolarmente bersagliata (come analizzato nella domanda precedente), è stata applicata una soglia dell'**80%** per questa nazione.

Il risultato di questa analisi è rappresentato nel seguente istogramma (*Figura 1.3*), dove gli attacchi dei gruppi individuati sono espressi in percentuale, suddivisi per nazione colpita.

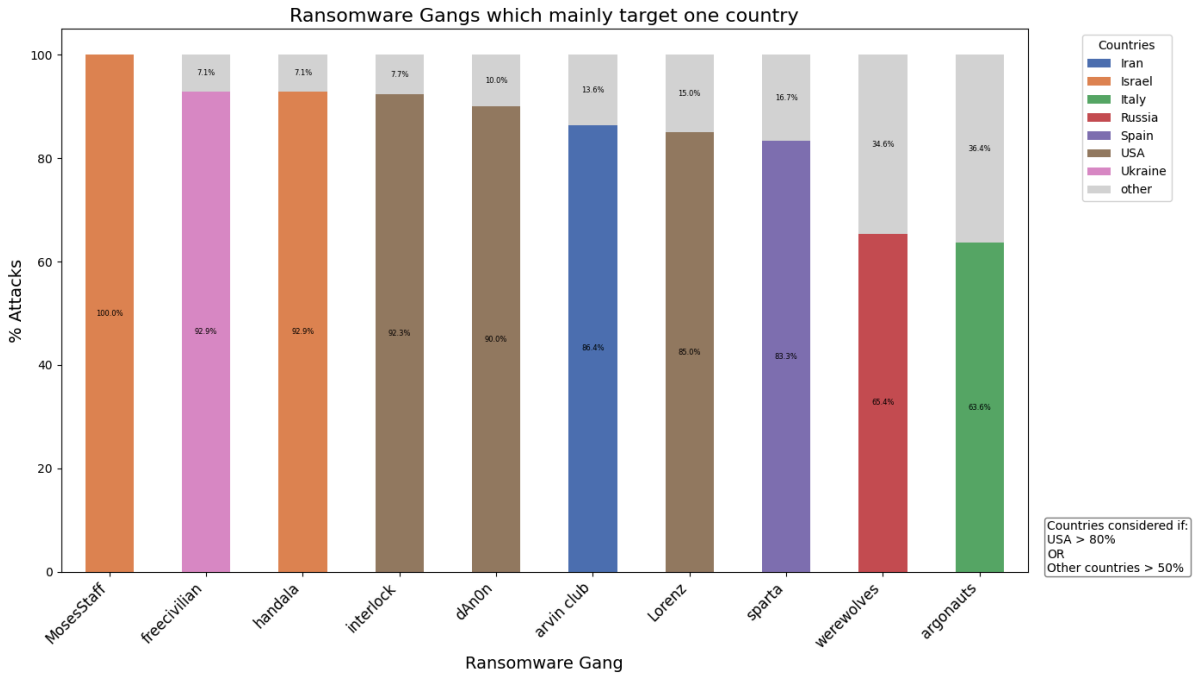

Figura 1.3: Distribuzione degli attacchi dei gruppi ransomware che colpiscono principalmente un paese.

La *Figura 1.3* evidenzia 10 gruppi ransomware. Per la maggior parte di questi gruppi, non emergono motivazioni chiare che giustifichino un particolare focus geografico.

Tuttavia, nel caso di **MosesStaff** e **Handala**, si tratta di gruppi che agiscono con motivazioni politiche legate ad ideologie anti-israeliane, come sarà approfondito nella *Domanda 8.2*.

Free Civilian, invece, ha guadagnato notorietà per l'intensificazione delle sue attività nel contesto del conflitto tra Russia e Ucraina. Questo gruppo è stato sospettato di agire sotto l'influenza o con il sostegno di attori russi, mirando a colpire obiettivi che riflettono le tensioni geopolitiche in corso.

2. Settori economici più colpiti

2.1: Quali settori economici sono più vulnerabili?

È stata analizzata la colonna "Victim Sector" del dataset con l'obiettivo di identificare i settori economici più colpiti dagli attacchi ransomware. Per ogni settore è stato calcolato il numero di attacchi subiti, permettendo di comprendere quale segmento dell'economia sia più vulnerabile a questa tipologia di crimine informatico. Successivamente sono state calcolate le percentuali di attacchi per ciascun settore, per poi essere rappresentate in un grafico a torta (*Figura 2.1*). Per migliorarne la leggibilità, i settori che hanno subito meno del 2% degli attacchi totali sono stati raggruppati nella categoria "Other".

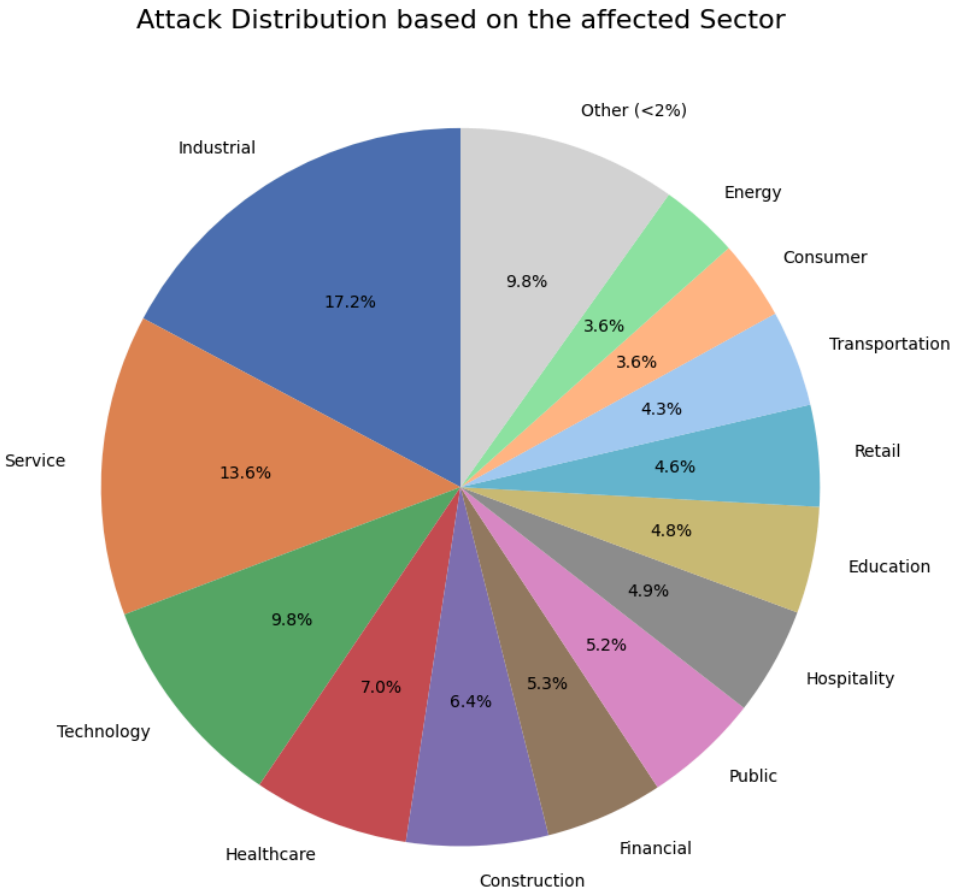

Figura 2.1: Distribuzione degli attacchi in base al settore colpito.

Dall'analisi emerge che, su un totale di 97 settori presi in considerazione, i tre settori più colpiti — **industria**, **servizi** e **tecnologie** — subiscono insieme il **40%** degli attacchi complessivi. Questo evidenzia come determinati settori, probabilmente per la loro centralità economica e la quantità di dati sensibili che gestiscono, siano diventati target privilegiati per i gruppi ransomware.

In particolare, il settore industriale, che include aziende manifatturiere e produttive, può essere particolarmente vulnerabile a causa della digitalizzazione dei processi produttivi e dell'integrazione di sistemi operativi critici che, se compromessi, possono causare gravi interruzioni. Il settore dei servizi, che comprende istituzioni finanziarie e altre aree chiave, è anch'esso frequentemente preso di mira, dato l'alto valore delle informazioni gestite. Infine, il settore delle tecnologie, che ospita numerose

aziende ad alta innovazione e con una grande esposizione a rischi digitali, risulta essere un obiettivo ricorrente per gli attacchi ransomware.

Per approfondire l'analisi, gli attacchi sono stati divisi per anno e rappresentati in diversi grafici a torta, uno per ciascun anno (*Figura 2.2*). Le distribuzioni non sono particolarmente differenti rispetto alla distribuzione generale, a parte un paio di eccezioni. Negli anni si può notare un aumento degli attacchi al settore dei servizi, e un calo al settore delle tecnologie.

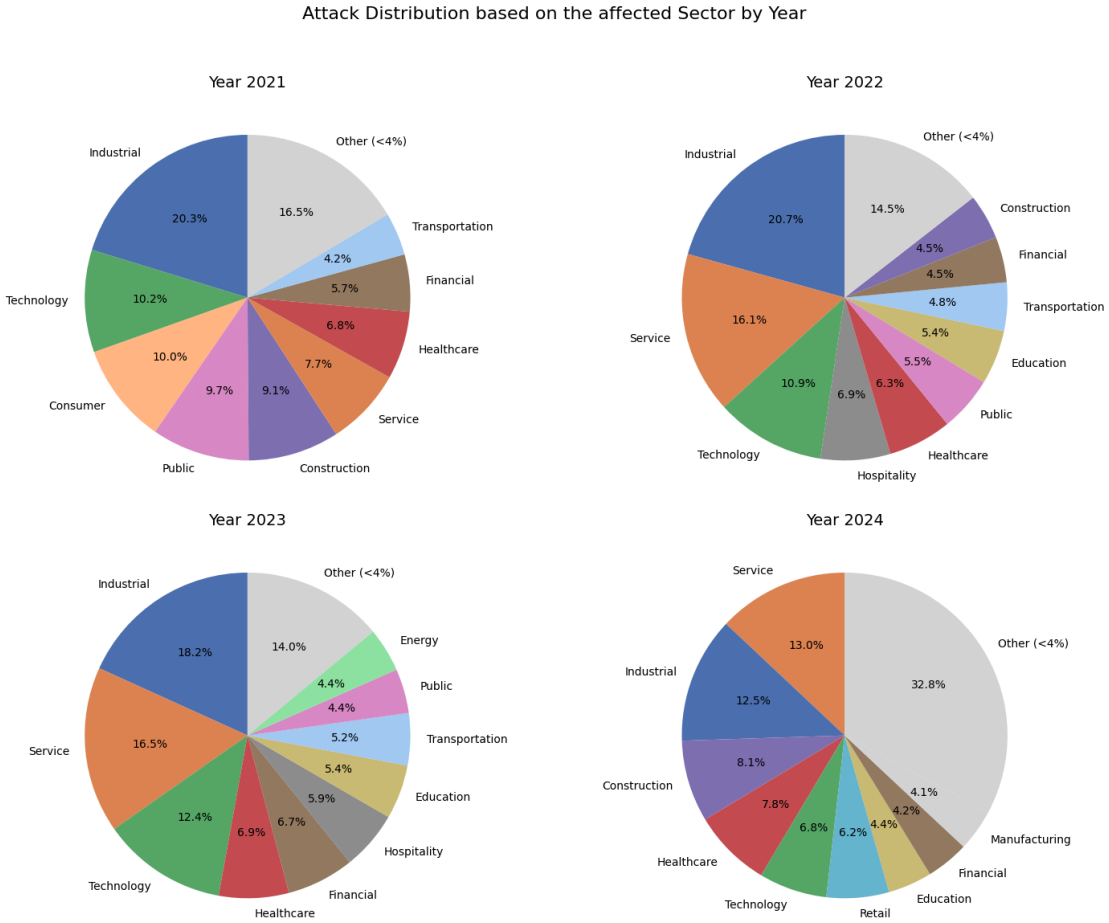

Figura 2.2: Distribuzione annuale degli attacchi in base al settore colpito.

2.2: I settori colpiti variano in base al gruppo ransomware?

L'analisi delle colonne "Gang" e "Victim Sector" è stata condotta sui 20 gruppi ransomware più attivi. La scelta di concentrarsi su questi gruppi è stata motivata dal desiderio di comprendere meglio le dinamiche e le preferenze specifiche dei gruppi che maggiormente influenzano il panorama delle minacce ransomware. Gli attacchi di ciascun gruppo sono stati raggruppati per settore colpito, convertiti in percentuali e rappresentati in un istogramma (*Figura 2.3*). Per una migliore leggibilità, i settori che hanno subito meno del 2% degli attacchi sono stati inclusi nella categoria "Other".

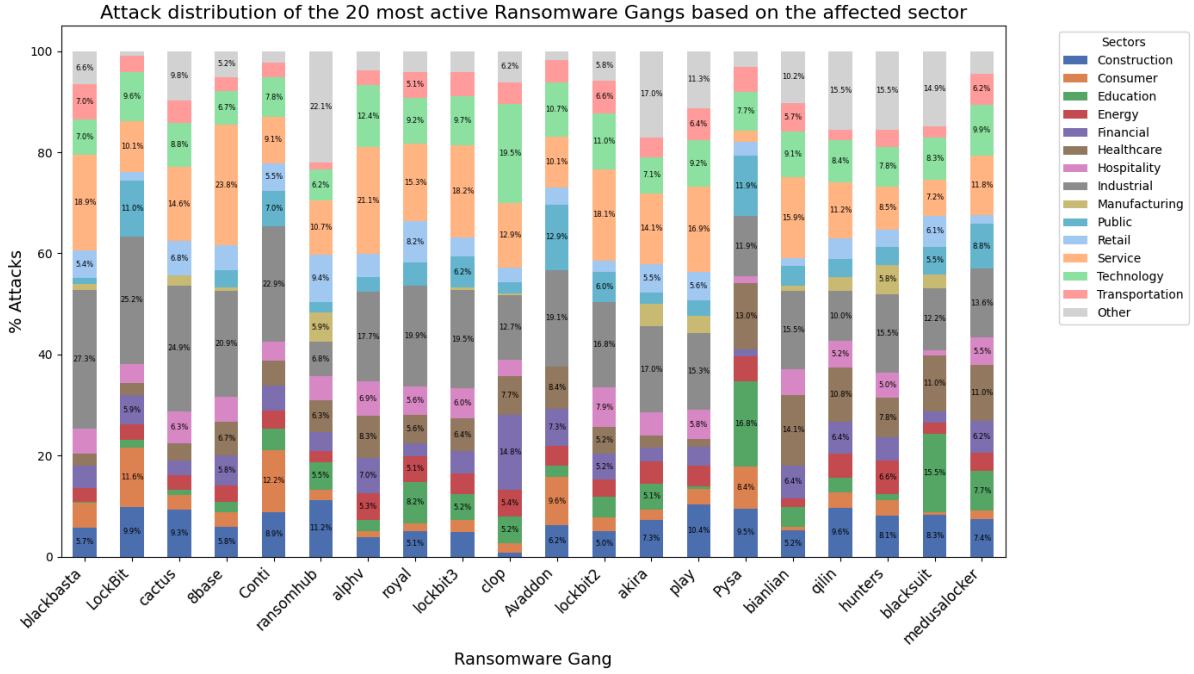

Figura 2.3: Distribuzione degli attacchi dei 20 gruppi ransomware più attivi in base al settore colpito.

Dall'analisi emergono alcune osservazioni importanti riguardo alla distribuzione degli attacchi tra i settori. In generale, la distribuzione degli attacchi tra i settori è risultata essere piuttosto uniforme, con alcune eccezioni significative che riflettono le preferenze operative di determinati gruppi. Ad esempio, il gruppo "RansomHub" si distingue per un comportamento anomalo, concentrandosi maggiormente su settori meno colpiti rispetto ad altri gruppi ransomware. D'altra parte, il gruppo "Pysa" ha mostrato una concentrazione di attacchi notevole nei settori della sanità e dell'istruzione, che sono tradizionalmente bersagli sensibili per motivi legati alla gestione di dati riservati e alla criticità dei servizi offerti.

3. Gruppi ransomware più attivi

3.1: Quali sono i gruppi ransomware più attivi in termini di numero di vittime?

Sono state analizzate le colonne "Gang" e "Victim" del dataset per identificare i gruppi ransomware più attivi e il numero di vittime associato a ciascun gruppo. Gli attacchi sono stati raggruppati per gruppo ransomware e per numero di vittime, e successivamente è stato creato un istogramma che rappresenta i dati relativi ai 20 gruppi più attivi (*Figura 3.1*). Questo approccio ha permesso di mettere in evidenza le differenze nella portata degli attacchi tra i vari gruppi.

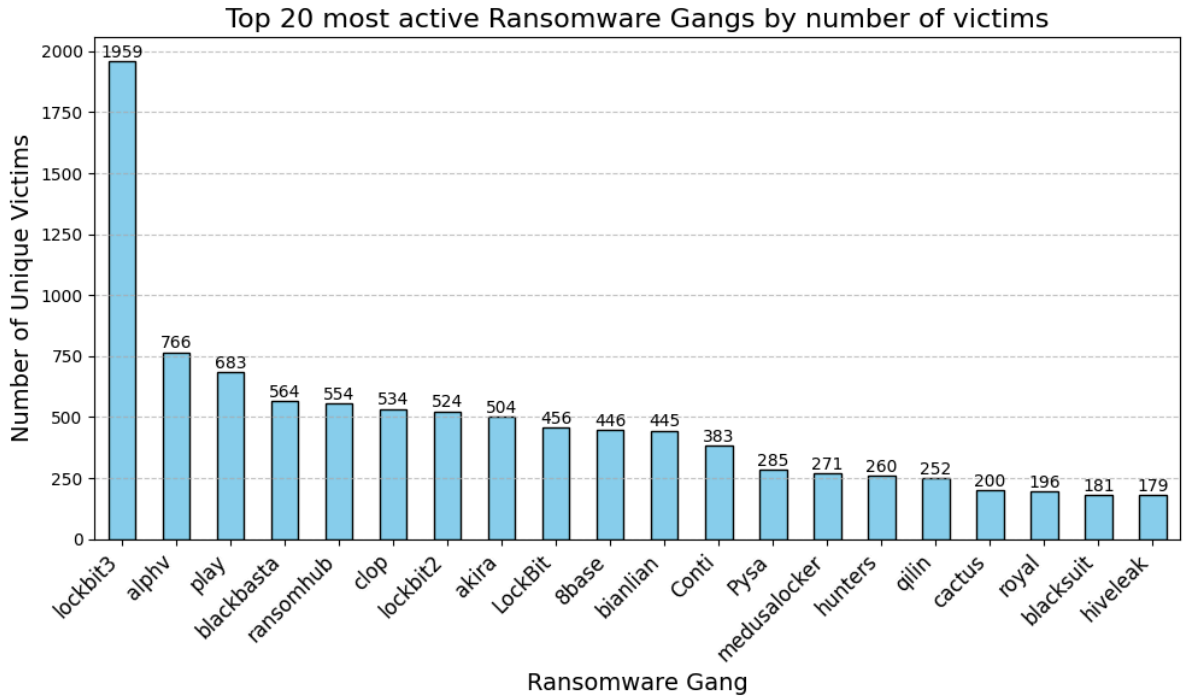

Figura 3.1: Numero di vittime dei 20 gruppi ransomware più attivi.

Dall'analisi emerge chiaramente che **LockBit3** è il gruppo più attivo, con un numero di vittime significativamente superiore rispetto agli altri. Per ottenere una comprensione più dettagliata dell'evoluzione delle attività dei gruppi ransomware, gli attacchi sono stati ulteriormente suddivisi per anno e rappresentati in quattro istogrammi distinti, uno per ciascun anno dal 2021 al 2024 (*Figura 3.2*).

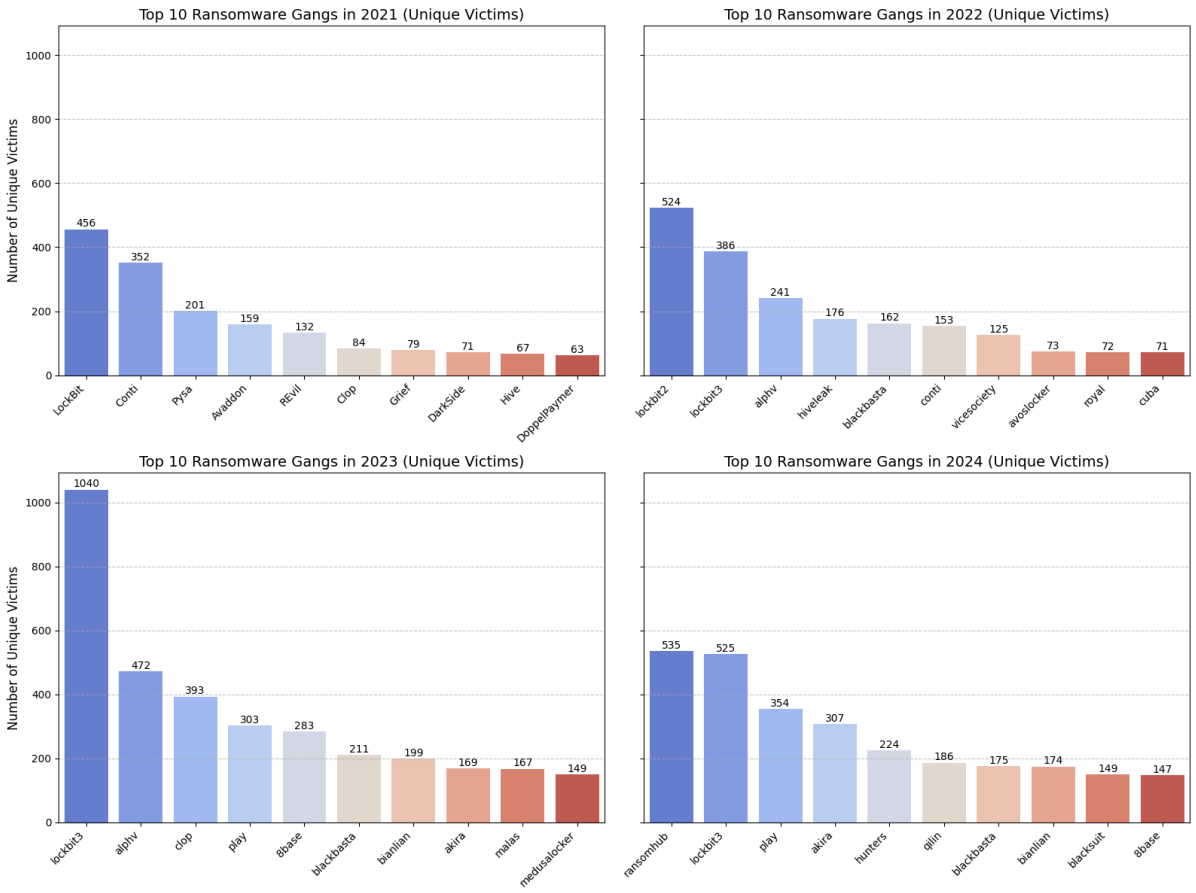

Figura 3.2: Numero di vittime dei 10 gruppi ransomware più attivi, divisi per ogni anno.

Dalla *Figura 3.2* sembra che i gruppi attivi cambino notevolmente da un anno all'altro. Tuttavia, un'analisi più approfondita suggerisce che questo cambiamento sia solo apparente, poiché molti di questi gruppi, pur adottando nuovi nomi, sono probabilmente formati dagli stessi membri di gruppi sciolti in precedenza.

Ad esempio:

- **Conti**, un gruppo noto per la sua attività aggressiva fino al 2022, ha ispirato la formazione di **Royal**, che ha continuato a condurre attacchi in modo simile.
- **REvil**, uno dei gruppi più attivi negli anni precedenti, è stato direttamente collegato alla nascita di **Black Basta**, un altro gruppo emergente che ha adottato tattiche simili.
- **LockBit**, invece, rappresenta un caso particolare. Questo gruppo ha introdotto diverse varianti, come **LockBit2** e **LockBit3**, dimostrando una notevole capacità di evolversi e adattarsi ai cambiamenti del panorama della sicurezza informatica.

Questa tendenza di riorganizzazione e rebranding dei gruppi ransomware è una strategia comune nel panorama delle minacce informatiche, spesso utilizzata per sfuggire alle indagini delle autorità o per adottare nuove tecnologie e tattiche. L'analisi temporale degli attacchi mette in evidenza non solo i cambiamenti nei gruppi attivi, ma anche le loro strategie di adattamento e resilienza.

3.2: Esistono gruppi che preferiscono colpire specifici settori o regioni?

L'analisi sulle regioni è stata già discussa precedentemente nella Domanda 1.2. Per quanto riguarda i gruppi ransomware che si concentrano su specifici settori, l'analisi delle colonne "Gang" e "Victim Country" del dataset ha permesso di identificare quelli con una chiara predilezione per determinati ambiti economici. L'analisi ha preso in considerazione esclusivamente i gruppi ransomware con un'attività significativa, definiti come quelli con più di 10 attacchi totali, e con **almeno il 40% degli attacchi concentrati in un unico settore**. Questa soglia è stata scelta per evidenziare quei gruppi che dimostrano una marcata specializzazione o preferenza nei loro target, rendendoli particolarmente rilevanti per l'analisi delle dinamiche settoriali. Nel seguente istogramma, gli attacchi di questi gruppi sono rappresentati in percentuale, suddivisi per settore colpito (*Figura 3.3*).

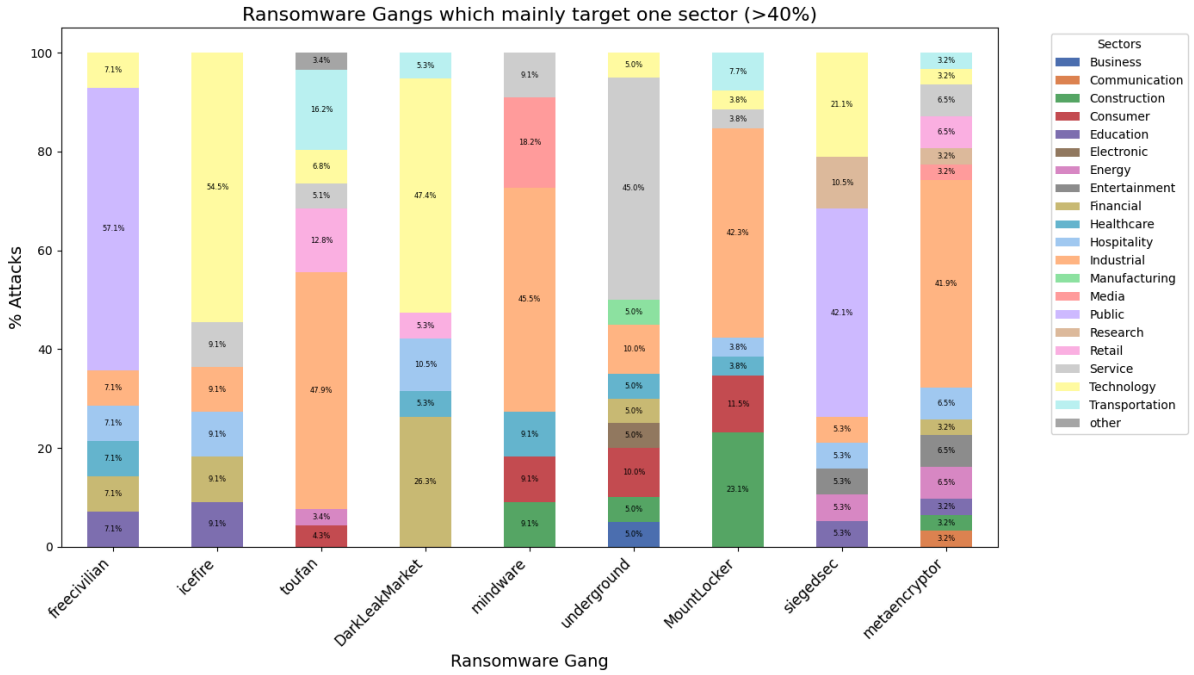

Figura 3.3: Distribuzione degli attacchi dei gruppi ransomware che colpiscono principalmente un settore.

L'analisi ha portato all'identificazione di 9 gruppi ransomware, di cui la maggior parte mostra una forte preferenza per settori che sono già noti come frequentemente bersagliati, come l'industria, i servizi e le tecnologie.

Tuttavia, spicca il gruppo **SiegedSec**, che emerge come un outlier per il suo particolare focus sul settore pubblico. Questo gruppo, infatti, è noto per le sue azioni di hacktivismo, con attacchi motivati politicamente. Un esempio significativo è l'attacco alla Heritage Foundation, un think tank conservatore statunitense, preso di mira per la sua posizione su temi come i diritti LGBTQ+ e l'aborto. Questo gruppo si distingue, quindi, non solo per la sua attività ransomware, ma anche per la sua componente ideologica, tipica degli hacktivisti, che rende i suoi attacchi mirati a specifiche ideologie politiche.

Inoltre, il gruppo **Free Civilian** emerge come un altro attore interessante, sebbene sia stato già trattato nella *Domanda 1.2.*

4. Temporalità degli attacchi

4.1: Gli attacchi sono aumentati o diminuiti nel tempo? Ci sono stagionalità o periodi dell'anno in cui gli attacchi sono più frequenti?

È stata analizzata la colonna "Date" del dataset per studiare la distribuzione temporale degli attacchi ransomware, raggruppandoli in base al periodo dell'anno in cui si sono verificati. Gli attacchi sono stati aggregati sia a granularità trimestrale che semestrale, consentendo di identificare pattern ricorrenti e variazioni stagionali nel corso del tempo. I risultati sono stati rappresentati nei seguenti istogrammi (*Figura 4.1*).

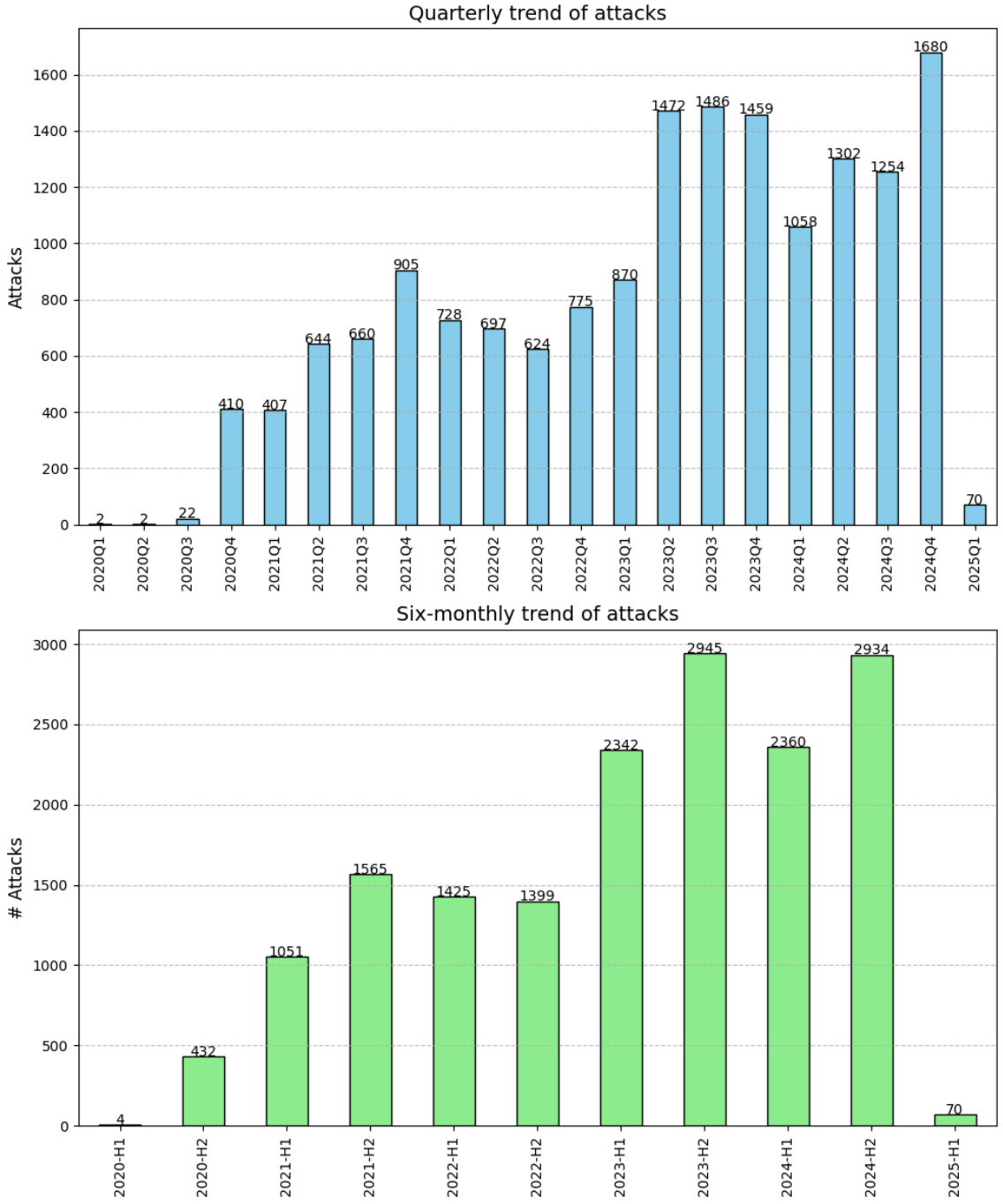

Figura 4.1: Andamento trimestrale e semestrale degli attacchi.

L’analisi mostra un aumento significativo del numero di attacchi nel tempo. In particolare, il numero di attacchi registrati nel 2024 è **più del doppio** rispetto a quello del 2021. Questo dato riflette non solo l’espansione delle attività dei gruppi ransomware, ma anche un possibile miglioramento nel monitoraggio e nella registrazione degli attacchi, rendendo il fenomeno sempre più evidente e preoccupante.

Un altro elemento interessante emerso dall'analisi è la distribuzione stagionale degli attacchi. In ciascun anno, **gli attacchi risultano più frequenti negli ultimi mesi**, suggerendo che i gruppi ransomware possano approfittare di periodi di minore attenzione o ridotta disponibilità di risorse da parte delle vittime. Questo fenomeno è particolarmente evidente durante il periodo delle festività, quando molte organizzazioni riducono le attività operative o dispongono di personale ridotto, rendendole più vulnerabili.

4.2: Esiste una correlazione tra gli attacchi ransomware e lo sfruttamento di CVE critiche?

Prima di condurre l'analisi, è stato necessario selezionare le CVE più critiche, basandosi su tre criteri principali:

1. **CVSS (Common Vulnerability Scoring System)**: È stato scelto un punteggio superiore a 9, indicando una vulnerabilità estremamente critica.
2. **EPSS (Exploit Prediction Scoring System)**: Sono state prese in considerazione solo le CVE con una probabilità di sfruttamento maggiore del 97%.
3. **Confermata associazione agli attacchi ransomware**: La scelta si è focalizzata sulle CVE per le quali esiste una conferma documentata del loro utilizzo in attacchi ransomware.

Sebbene molte vulnerabilità rispettassero questi criteri, sono state selezionate manualmente le 4 CVE ritenute più rilevanti per il panorama ransomware. Per ciascuna CVE è stato creato un grafico a linee che mostra l'andamento giornaliero degli attacchi nei 14 giorni intorno alla data di scoperta della vulnerabilità (*Figura 4.2*).

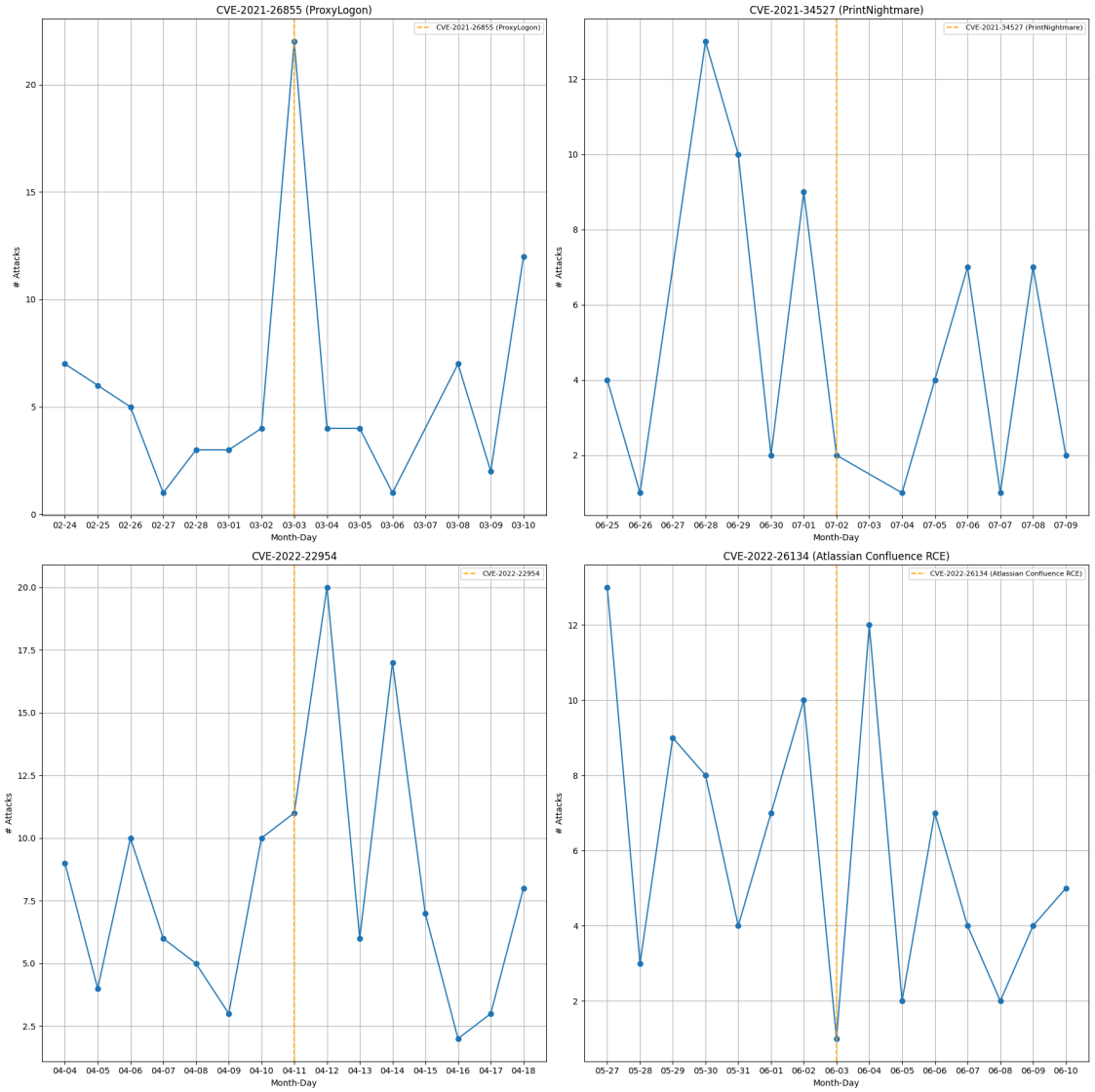

Figura 4.2: Andamento temporale degli attacchi nei 14 giorni intorno alla data di scoperta della CVE.

Dall'analisi è emerso che il picco degli attacchi non coincide sempre con la data di pubblicazione ufficiale della CVE. Questo è dovuto a due fattori principali:

- **Sfruttamento pre-pubblicazione:** molte vulnerabilità vengono sfruttate prima della divulgazione ufficiale, evidenziando la discrepanza tra la data di scoperta e quella di pubblicazione.
- **Sfruttamento post-patch:** i picchi di attacchi possono verificarsi anche dopo il rilascio delle patch, probabilmente a causa del ritardo nell'applicazione delle correzioni da parte delle organizzazioni.

Di seguito sono illustrate le vulnerabilità analizzate nel dettaglio:

- La vulnerabilità **CVE-2021-26855**, nota anche come "**ProxyLogon**", è una grave falla di sicurezza nei server **Microsoft Exchange** che consente a un attaccante non autenticato di eseguire codice arbitrario sul server. Questa vulnerabilità sfrutta un difetto nel meccanismo di autenticazione di Exchange, permettendo all'attaccante di impersonare un amministratore e accedere al sistema senza necessità di credenziali valide. La vulnerabilità è stata risolta da Microsoft il 2 marzo 2021 con il rilascio di una patch di sicurezza. Tra i gruppi principali che l'hanno utilizzata ci sono: REvil, Clop, Conti, ALPHV e Babuk.

- La vulnerabilità **CVE-2021-34527**, nota anche come "**PrintNightmare",** è una vulnerabilità di esecuzione di codice remoto (RCE) e di elevazione dei privilegi che interessa il servizio **Windows Print Spooler**, presente in tutte le versioni di Windows. È stata sfruttata da vari gruppi ransomware, come per esempio Conti, LockBit e Vice Society. Per difendersi da attacchi basati su PrintNightmare, Microsoft ha rilasciato patch di sicurezza a partire da luglio 2021.

- La vulnerabilità **CVE-2022-22954** riguarda **VMware Workspace ONE Access** e consente l'esecuzione remota di codice a causa di un'iniezione di template lato server. Un attaccante malintenzionato con accesso di rete può sfruttare questa vulnerabilità per eseguire comandi arbitrari sul sistema vulnerabile. La vulnerabilità è stata risolta il 6 aprile 2022 con la pubblicazione dell'advisory VMSA-2022-0011 da parte di VMware. È stata sfruttata da gruppi come LockBit, Conti, Alphv, RansomEXX e Cuba Ransomware.

- La vulnerabilità **CVE-2022-26134** è una grave falla di esecuzione remota di codice (RCE) non autenticata che interessa le versioni supportate di Confluence Server e Data Center. Questa vulnerabilità consente a un attaccante di eseguire codice arbitrario su un'istanza vulnerabile di Confluence. La vulnerabilità è stata risolta da Atlassian il 3 giugno 2022. Tale CVE è stata sfruttata dal gruppo AvosLocker.

5. Analisi sulle vittime

5.1: Qual è il numero medio di dipendenti o il fatturato delle aziende colpite?

Sono state analizzate le colonne "Number of Employees" e "Sales" del dataset, disponibili esclusivamente per gli attacchi registrati a partire dal 2024. Poiché i dati spesso riportano intervalli di valori per il numero di dipendenti o il fatturato, le informazioni sono state raggruppate in sei categorie distinte per ciascuna variabile. I valori espressi in valute differenti sono stati convertiti in dollari. Questo approccio ha permesso di individuare le fasce aziendali maggiormente colpite in termini di dimensioni e fatturato (*Figura 5.1*).

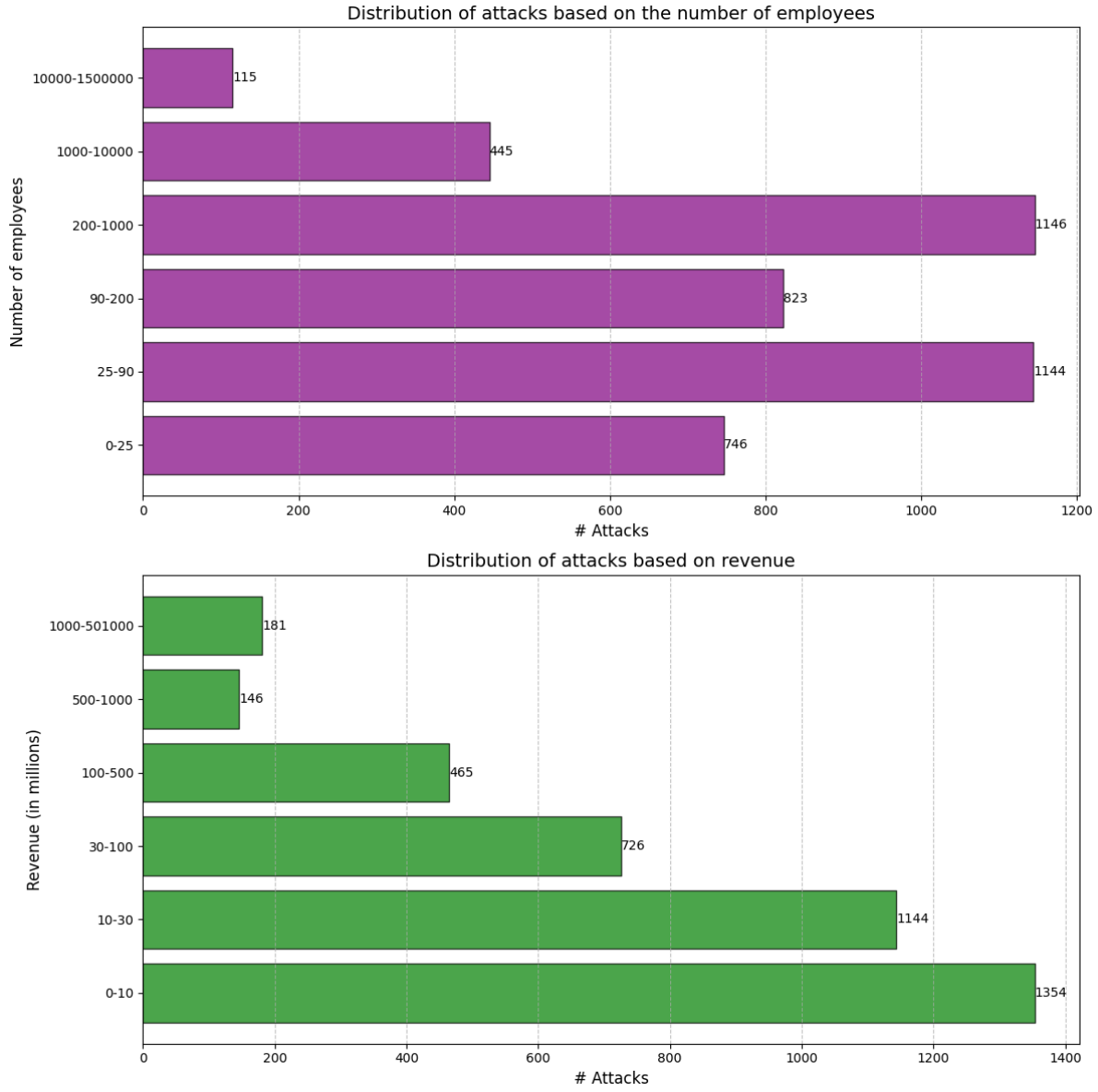

Figura 5.1: Distribuzione degli attacchi in base al numero di dipendenti e al fatturato delle aziende colpite.

Dall’analisi emerge che:

- Le aziende con un numero di dipendenti compreso tra 25 e 1.000 rappresentano il **70,5%** degli attacchi totali.
- In termini di fatturato, le imprese con ricavi compresi tra 1 e 30 milioni di euro costituiscono il **62,2%** degli attacchi.

Questi dati evidenziano una chiara preferenza dei gruppi ransomware per le aziende di piccole e medie dimensioni (PMI). Questo comportamento può essere spiegato da diversi fattori:

- **Maggiore vulnerabilità**: Le PMI, rispetto alle grandi aziende, spesso non dispongono delle risorse economiche e tecnologiche necessarie per implementare soluzioni avanzate di sicurezza informatica. Questa lacuna le rende bersagli più facili per gli attaccanti.
- **Elevata pressione per il pagamento**: Le PMI, a differenza delle grandi imprese, possono subire un impatto devastante anche da brevi interruzioni operative. Di conseguenza, queste aziende potrebbero essere più inclini a pagare il riscatto per ripristinare rapidamente le loro attività.
- **Minore attenzione alla cybersecurity**: La percezione del rischio è spesso meno sviluppata nelle PMI, che tendono a investire meno in formazione e protezione rispetto alle grandi aziende.

I risultati sottolineano l’urgenza di sensibilizzare le PMI sull'importanza della sicurezza informatica. Nonostante le risorse limitate, è fondamentale che queste aziende investano in misure preventive, come backup regolari, monitoraggio delle reti e formazione del personale.

5.2: Le vittime di un determinato gruppo condividono attributi simili?

Sono state analizzate le colonne "Gang", "Victim Country" e "Victim Sector" del dataset, con un focus sui 10 gruppi ransomware più attivi. L'obiettivo è stato quello di identificare i settori economici e le nazioni maggiormente colpite da ciascun gruppo. I dati sono stati rappresentati in un istogramma che illustra il numero di attacchi condotti da ogni gruppo, suddivisi per paese e settore delle vittime. Per migliorarne la leggibilità, le combinazioni paese-settore che rappresentano meno dello 0,15% degli attacchi totali sono state raggruppate nella categoria "Other" (*Figura 5.2*).

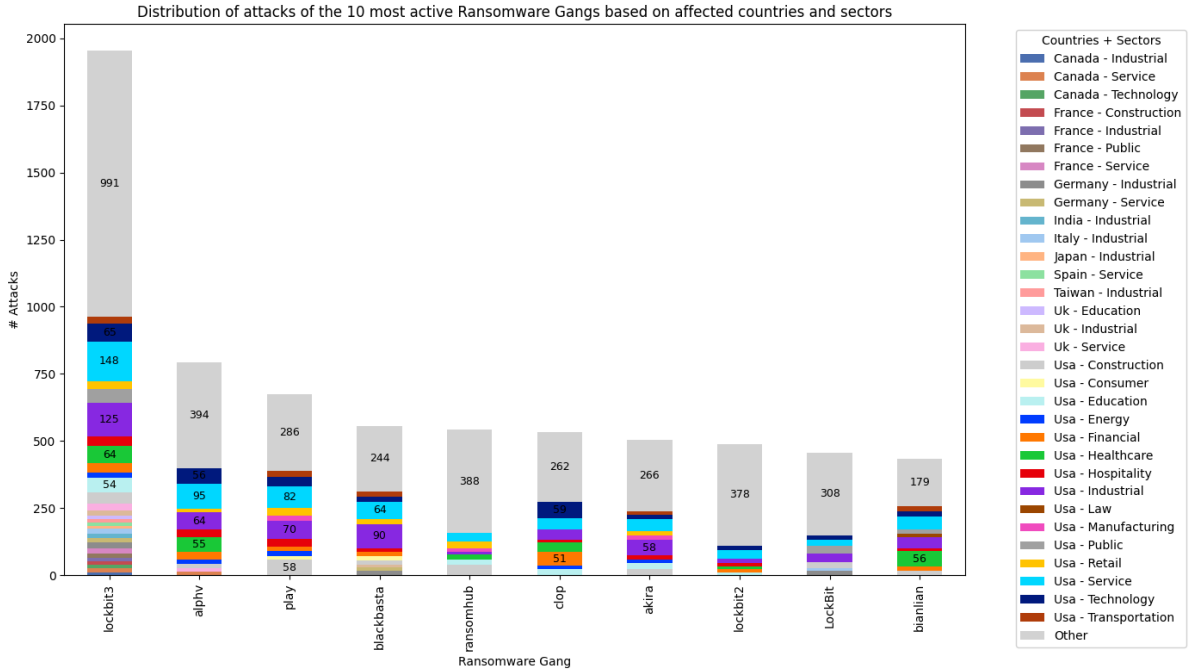

Figura 5.2: Distribuzione degli attacchi dei 10 gruppi ransomware più attivi in base al settore e al paese colpito.

Dalla *Figura 5.2* emergono alcune considerazioni rilevanti:

- **Conferma di tendenze generali**: Come già evidenziato in analisi precedenti, le vittime tendono a concentrarsi nei paesi e nei settori più frequentemente presi di mira dai gruppi ransomware. Tra questi spiccano gli Stati Uniti e i settori industriale, tecnologico e dei servizi.
- **Eterogeneità delle vittime:** L'analisi evidenzia che i gruppi ransomware più attivi tendono a colpire una gamma molto ampia di vittime, distribuite tra diversi paesi e settori. La maggior parte di essi adotta una strategia altamente diversificata, mirata a massimizzare le opportunità di successo e ampliare il proprio raggio d'azione.

5.3: Esistono vittime colpite più volte? Quali?

È stata analizzata la colonna "Victim" del dataset, contando il numero di occorrenze per ciascuna vittima. Un istogramma è stato creato per mostrare, in percentuale, il numero di attacchi subiti dalle varie vittime. (*Figura 5.3*)

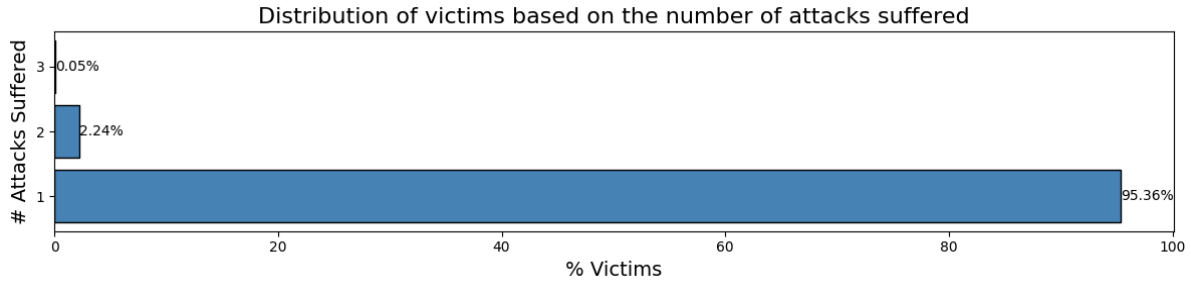

Figura 5.3: Distribuzione delle vittime in base alla numero di attacchi subiti.

L'analisi ha evidenziato che è raro che una vittima venga colpita più volte: questo fenomeno si verifica per **poco più del 2%** delle vittime, mentre solo lo 0,05% è stato colpito tre volte. Queste ultime sono rappresentate nel seguente istogramma (*Figura 5.4*).

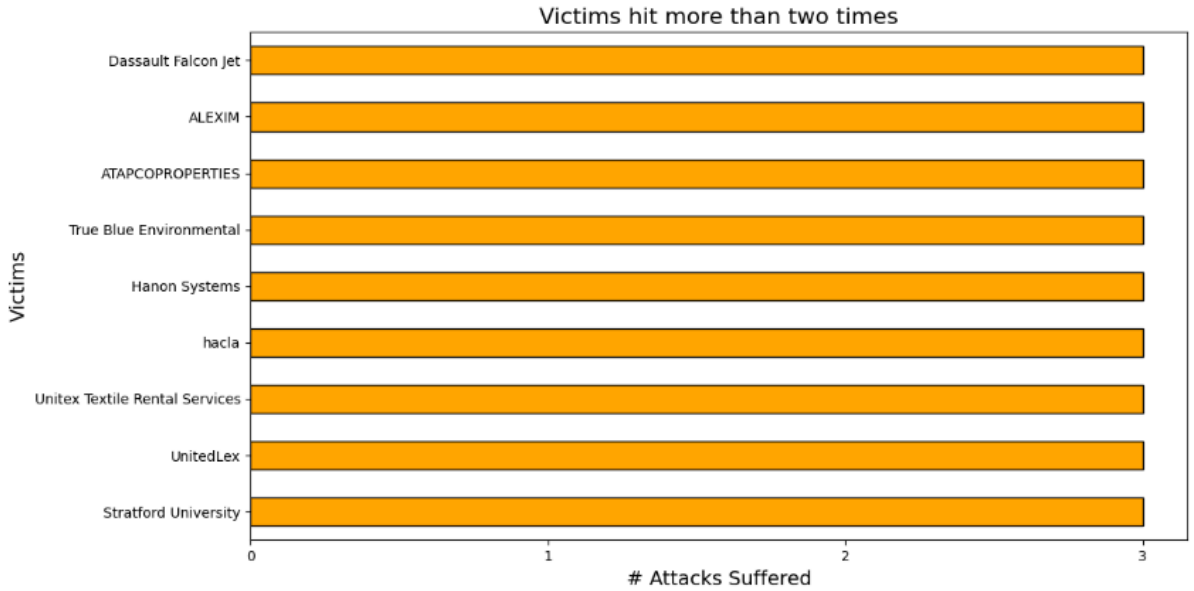

Figura 5.4: Vittime colpite più di due volte.

Le possibili cause di un attacco ripetuto alla stessa vittima sono varie, tra cui:

- **Vulnerabilità persistenti**: Se le debolezze nei sistemi non vengono corrette dopo il primo attacco, gli aggressori possono approfittarne per lanciare attacchi successivi (come potrebbe essere accaduto ad Alexim, che è stata colpita tre volte in pochi mesi dal gruppo ransomware Clop).

- **Targeting strategico**: Come già analizzato nella domanda 2.1, settori come l'industria e le tecnologie rappresentano obiettivi strategici per i gruppi ransomware, aumentando il rischio di attacchi ripetuti (più della metà di queste vittime operano in questi settori).

- **Pagamento dei riscatti**: Se un'organizzazione paga un riscatto, può essere percepita come più incline a soddisfare le richieste degli aggressori, aumentando la probabilità di nuovi attacchi.

- **Accesso continuato**: Gli aggressori potrebbero mantenere un accesso persistente ai sistemi compromessi, ripetendo gli attacchi per sfruttare ulteriormente i dati rubati o per fare pressione sul pagamento del riscatto.

6. Relazioni tra variabili

6.1: La frequenza degli attacchi in un paese è correlata al settore economico predominante?

Sono state analizzate le colonne "Victim Country" e "Victim Sector" del dataset, concentrandosi sulle nazioni che hanno subito almeno il 2% degli attacchi totali. È stato creato un istogramma che mostra, in percentuale, il numero di attacchi ricevuti da ciascuna nazione, con una suddivisione per settore colpito. Per migliorare la leggibilità del grafico, i settori che hanno subito meno dell'1% degli attacchi totali sono stati raggruppati nella categoria "Other" (*Figura 6.1*).

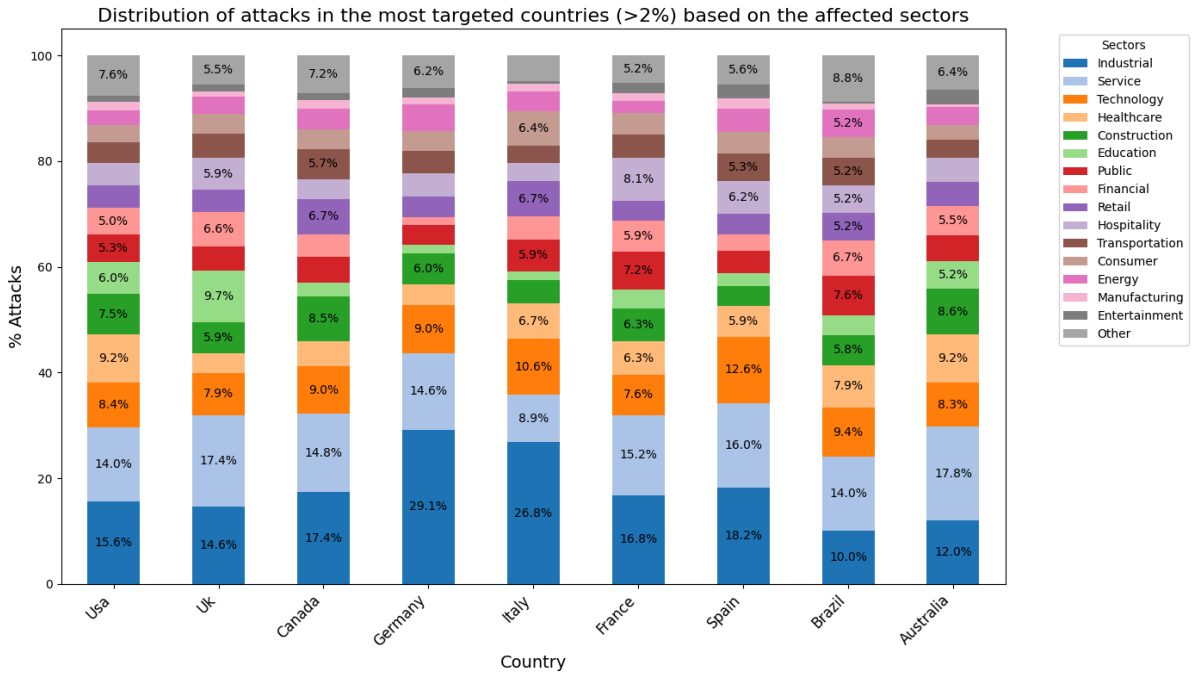

Figura 6.1: Distribuzione degli attacchi alle nazioni più colpite, in base al settore colpito.

Dalla *Figura 6.1* emerge chiaramente che, in ogni nazione, i settori più colpiti dagli attacchi ransomware sono l'industria, i servizi e le tecnologie, confermandosi tra i target principali dei gruppi ransomware. Le nazioni maggiormente colpite, infatti, sono quelle in cui questi settori sono altamente sviluppati e rappresentano una componente cruciale del tessuto economico e produttivo. Questo evidenzia una chiara correlazione tra il livello di sviluppo economico di un paese e la frequenza degli attacchi ransomware, con una maggiore esposizione delle economie avanzate.

6.2: Esistono pattern ricorrenti tra gruppi ransomware, settori e paesi?

Sono state analizzate le colonne "Gang", "Victim Sector" e "Victim Country" del dataset, raggruppando gli attacchi in base alle triplette "gruppo ransomware - nazione - settore". È stato creato un istogramma che rappresenta le triplette che compaiono almeno 60 volte (*Figura 6.2*).

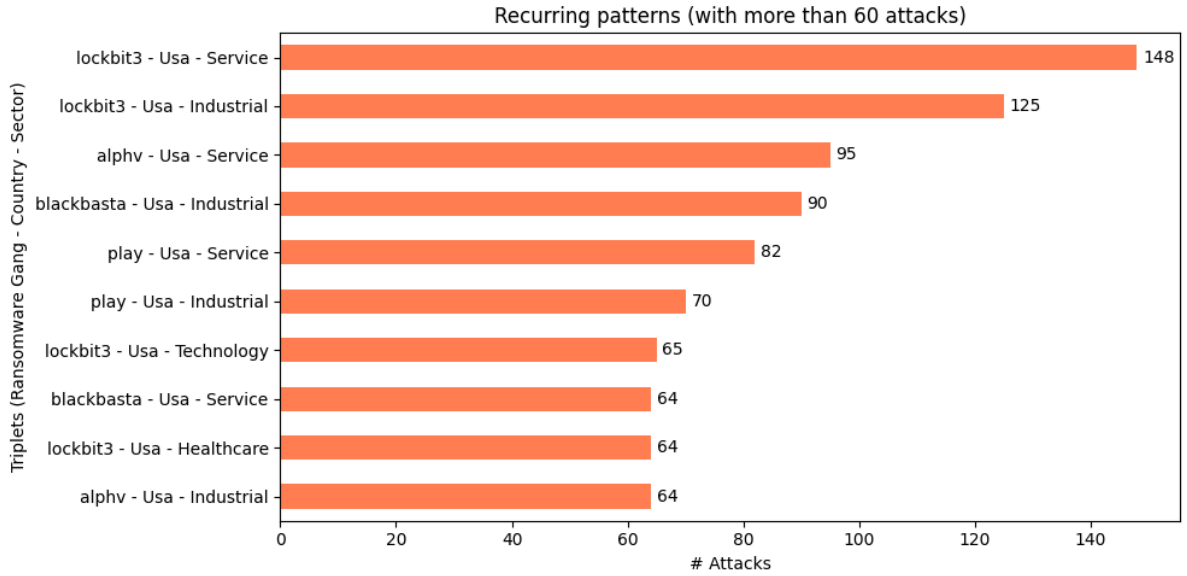

Figura 6.2: Pattern ricorrenti (gruppo ransomware - nazione - settore), ovvero con più di 60 attacchi subiti.

Dalla *Figura 6.2* emerge che i gruppi ransomware più attivi tendono a colpire principalmente i settori e i paesi più frequentemente bersagliati, creando combinazioni ricorrenti. Come ci si poteva aspettare, gli Stati Uniti, che concentrano circa la metà degli attacchi totali, compaiono in tutte le triplette analizzate nella prima rappresentazione.

Per un'analisi più approfondita, è stato realizzato un secondo istogramma che esclude le triplette contenenti gli Stati Uniti e include solo quelle che compaiono almeno 20 volte (*Figura 6.3*). Questo approccio consente di esaminare le relazioni tra gruppi ransomware, settori e nazioni al di fuori del contesto statunitense, mettendo in evidenza combinazioni significative che sarebbero state altrimenti sovrastate dal peso degli attacchi diretti agli USA.

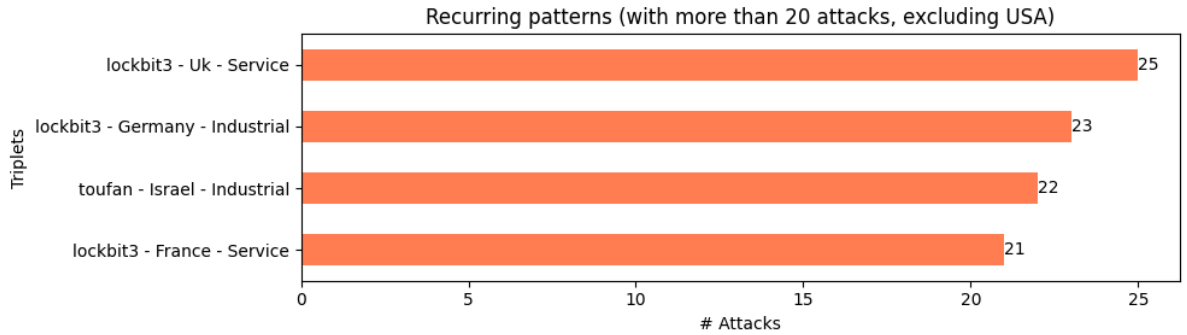

Figura 6.3: Pattern ricorrenti (con più di 20 attacchi subiti), escludendo gli Stati Uniti.

Anche dalla *Figura 6.3* non emergono pattern particolari, ma piuttosto una conferma delle tendenze generali, con una preferenza per attaccare le nazioni e i settori più colpiti.

7. Analisi di outlier

7.1: Ci sono stati periodi con un numero elevato di attacchi in breve tempo?

Gli attacchi nel tempo sono stati rappresentati in un grafico a linee con granularità settimanale (*Figura 7.1*).

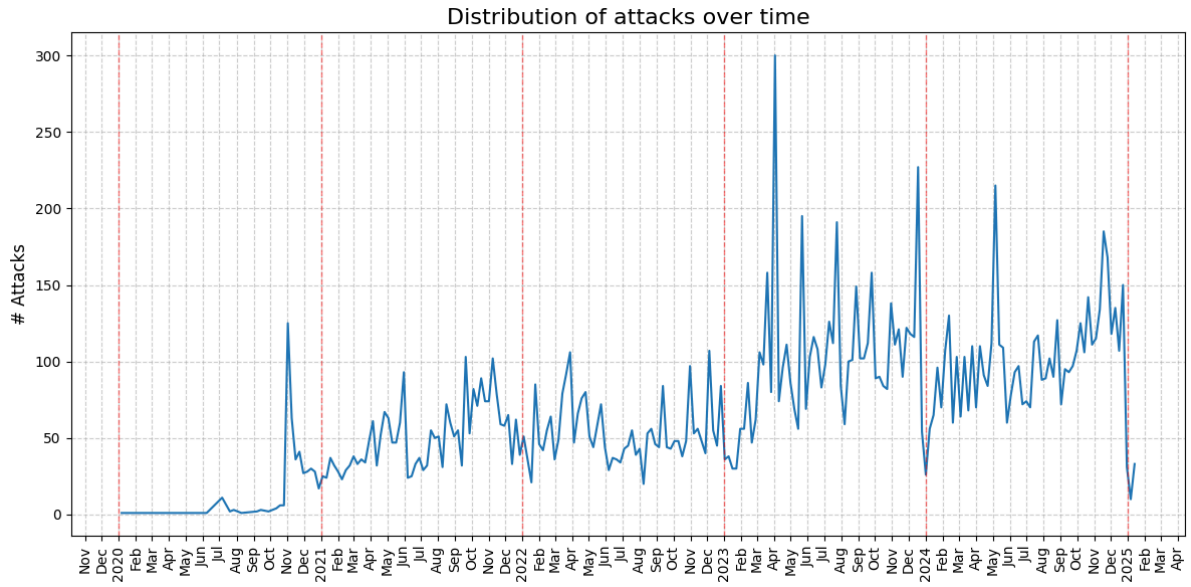

Figura 7.1: Andamento temporale degli attacchi a granularità settimanale.

Dalla *Figura 7.1* si notano alcune settimane con un numero significativamente elevato di attacchi, come all'inizio di aprile 2023, a metà dicembre 2023 e all'inizio di maggio 2024. Questi picchi sono approfonditi nelle domande 4.2 e 8.1. Inoltre, come discusso nella domanda 4.1, si evidenzia una crescita generale dell'attività ransomware a partire dal 2023.

7.2: Quali gruppi hanno effettuato un numero elevato di attacchi in breve tempo?

Sono state analizzate le colonne "Gang" e "Date" del dataset, concentrandosi sugli attacchi verificatisi dal 2023 in poi. Questo principalmente per due motivi: da un lato, negli ultimi anni si è registrato un significativo aumento del numero di attacchi, dall'altro, per migliorare la leggibilità del grafico. L'istogramma seguente mostra, mese per mese, gli attacchi compiuti dalle gang che hanno effettuato **almeno 50 attacchi** in quel mese (*Figura 7.2*).

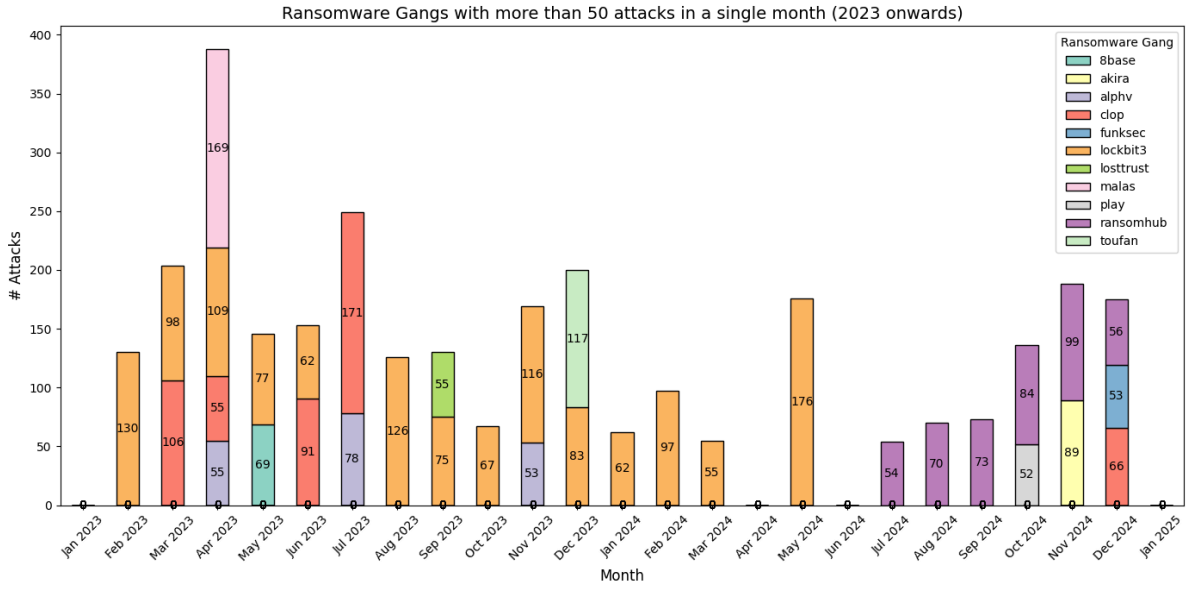

Figura 7.2: Gruppi ransomware con più di 50 attacchi in un singolo mese (dal 2023 in poi).

Dal grafico emergono chiaramente i gruppi più attivi, come **LockBit** e **RansomHub**. Quest'ultimo, nato a febbraio 2024, ha registrato una notevole crescita nella seconda metà del 2024, superando in numero di attacchi anche LockBit in alcuni mesi.

Oltre a questi gruppi, si evidenziano alcune situazioni particolari, come i 169 attacchi del gruppo hacktivist **Malas** nell'aprile 2023. A differenza di altri gruppi, Malas non richiedeva il pagamento di un riscatto, ma chiedeva che l'importo fosse donato a una delle associazioni benefiche proposte dal gruppo. Questo comportamento, raro nel panorama del ransomware, suggerisce un uso della tecnica per fini ideologici piuttosto che puramente economici.

Un altro caso interessante riguarda il gruppo pro-palestina **Toufan**, che ha compiuto 117 attacchi nel mese di dicembre 2023, periodo in cui il conflitto tra Israele e Palestina si è intensificato. Questo evidenzia una correlazione diretta tra eventi geopolitici e l'attività di alcune gang, sottolineando come il ransomware venga utilizzato anche come strumento di protesta politica.

8. Rischio geopolitico

8.1: Le attività di determinati gruppi aumentano in relazione a eventi politici o economici?

Gli attacchi nel tempo sono stati rappresentati in un grafico a linee con granularità mensile, nel quale sono stati evidenziati alcuni dei principali eventi politici degli ultimi anni: l'invasione russa dell'Ucraina, l'adesione della Finlandia alla NATO, l'attacco di Hamas a Israele e le elezioni presidenziali statunitensi del 2024 (*Figura 8.1*).

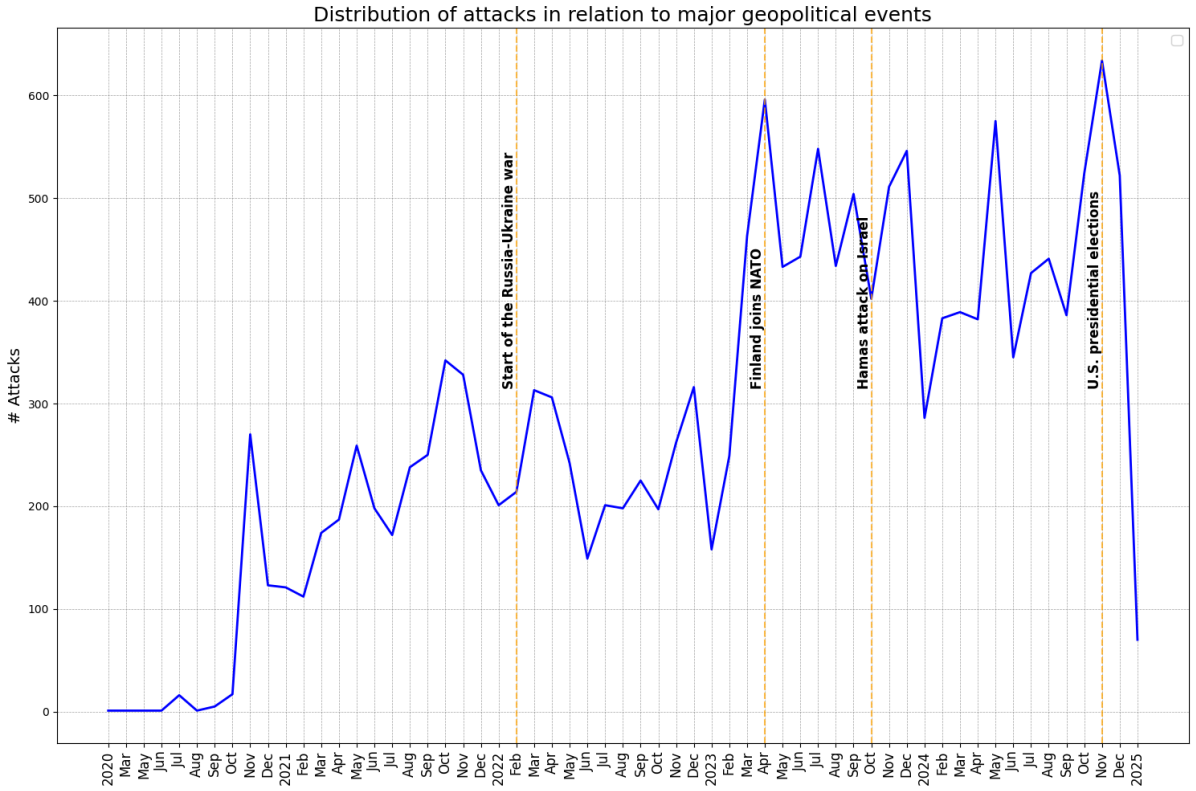

Figura 8.1: Distribuzione degli attacchi in relazione ai maggiori eventi geopolitici degli ultimi anni.

Si osserva frequentemente un aumento degli attacchi generali in corrispondenza di questi eventi, ma è difficile determinare quanto siano effettivamente correlati senza un'analisi più approfondita. Per questo motivo, si è deciso di esaminare gli attacchi mirati ai paesi coinvolti in ciascuno di questi eventi, rappresentandoli in un istogramma che copre un intervallo di 6 mesi attorno a ciascun evento (*Figura 8.2*). Questo approccio consente di analizzare meglio le fluttuazioni specifiche che potrebbero essere legate a eventi politici significativi.

Un'eccezione è stata fatta per la guerra russo-ucraina, poiché non ci sono sufficienti dati relativi a questi paesi nel periodo specificato. Tuttavia, dopo aver effettuato una ricerca sull'argomento, è stato riscontrato che il picco di attacchi a ottobre 2021 è altamente probabile che sia correlato, considerando che gli attacchi informatici verso l'Ucraina sono iniziati molto prima dell'inizio del conflitto, proprio nell'ottobre 2021.

Sono stati esaminati gli attacchi informatici diretti ai seguenti paesi in relazione agli eventi politici considerati:

- Gli attacchi ai paesi della NATO in seguito all'adesione della Finlandia all'alleanza.
- Gli attacchi a Israele in seguito all'attacco di Hamas.
- Gli attacchi agli Stati Uniti dopo le elezioni presidenziali.

Figura 8.2: Distribuzione degli attacchi rivolti ai paesi coinvolti nei maggiori eventi politici degli ultimi anni.

Da questi grafici si nota un evidente aumento degli attacchi nei mesi successivi agli eventi, confermando l'ipotesi che l'attività di alcuni gruppi ransomware sia strettamente collegata al panorama politico. È evidente che gli attacchi informatici siano utilizzati come una tattica complementare alle operazioni politiche o militari più tradizionali.

8.2: Esistono connessioni tra gruppi ransomware e stati nazionali?

Per analizzare eventuali connessioni tra gruppi ransomware e stati nazionali, sono state prese in considerazione le colonne "Gang" e "Victim Country" del dataset. Si è ipotizzato che, qualora un gruppo ransomware operasse per conto di uno stato, i suoi attacchi sarebbero concentrati su un numero limitato di paesi. Partendo da questa ipotesi, sono stati analizzati i gruppi ransomware con almeno 10 attacchi totali distribuiti su un **massimo di 8 paesi diversi**. Gli attacchi di ciascun gruppo sono stati rappresentati in un istogramma, suddivisi per nazione colpita e mostrati in percentuale (*Figura 8.3*). Inoltre, utilizzando le informazioni presenti nella sezione "Ransomware Gang Profile" del dataset, è stata identificata la presunta nazione di provenienza di alcuni gruppi ransomware. Sono stati esclusi dall'analisi i gruppi per cui mancavano informazioni sufficienti sulla loro origine.

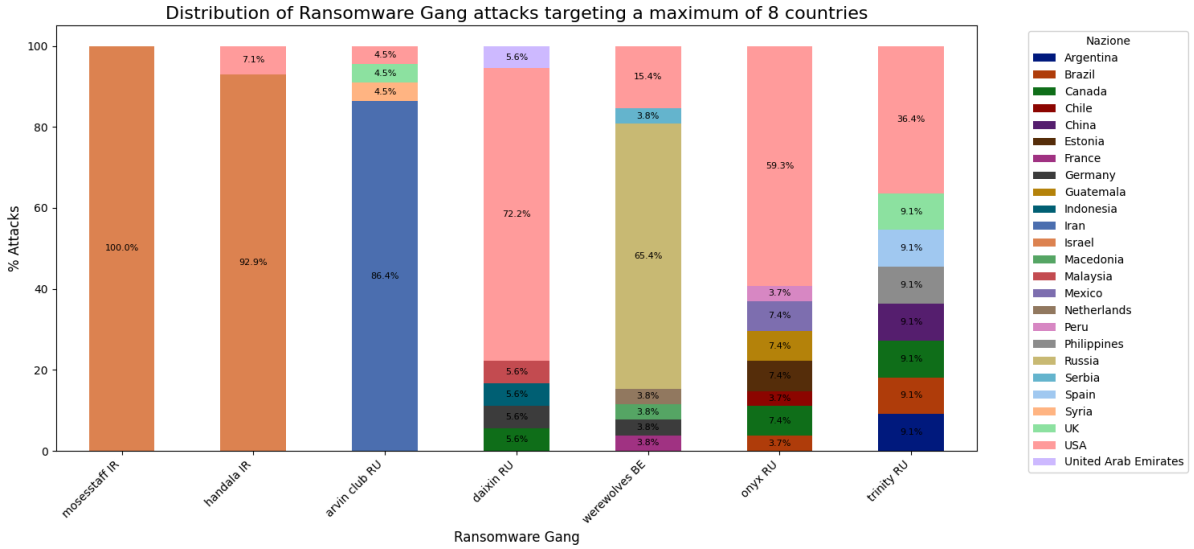

Figura 8.3: Distribuzione degli attacchi dei gruppi ransomware che colpiscono un massimo di otto paesi diversi

Dal grafico emergono gruppi come **MosesStaff** e **Handala**, che concentrano quasi tutti i loro attacchi verso Israele. Questi gruppi sono sospettati di operare per conto dello stato iraniano, non solo per la specifica scelta dei loro obiettivi, ma anche per la natura stessa dei loro attacchi. A differenza di molti altri gruppi ransomware, che mirano a guadagnare denaro attraverso il pagamento di riscatti, MosesStaff e Handala non richiedono riscatti. Invece, si concentrano sul causare il maggior danno possibile attraverso il furto e la pubblicazione di dati sensibili, rafforzando l'ipotesi di un movente politico o geopolitico.

Per quanto riguarda i gruppi russi come **Daixin**, **Onyx** e **Trinity**, la situazione è meno chiara. Questi gruppi tendono a colpire prevalentemente obiettivi in stati occidentali, il che potrebbe teoricamente allinearsi agli interessi geopolitici della Russia. Tuttavia, a differenza di MosesStaff e Handala, gli attacchi di Daixin, Onyx e Trinity sembrano avere principalmente fini economici, con richieste di riscatto chiare. Al momento, non esistono prove dirette che colleghino questi gruppi al governo russo. È possibile che operino in modo indipendente, approfittando di un ecosistema favorevole in Russia, dove le autorità sembrano tollerare (o ignorare) le loro attività, purché non colpiscano obiettivi nazionali o alleati.

Conclusioni

In conclusione, l'analisi condotta ha confermato che gli attacchi ransomware continuano a rappresentare una minaccia crescente e sempre più sofisticata per le organizzazioni globali. I risultati evidenziano una forte concentrazione geografica delle vittime, con gli Stati Uniti come paese più colpito, seguiti da altre economie avanzate. I settori industriale, dei servizi e delle tecnologie si rivelano i più vulnerabili, rappresentando i principali target dei gruppi ransomware. In particolare, le piccole e medie imprese (PMI) risultano le più vulnerabili, poiché spesso dispongono di risorse limitate per implementare adeguate misure di sicurezza, rendendole obiettivi privilegiati per gli attaccanti.

Negli ultimi anni, gli attacchi ransomware hanno visto un incremento significativo, con un trend in costante crescita che ha portato a un raddoppio degli attacchi dal 2021 al 2024. L'analisi ha anche rilevato una stagionalità nelle incursioni, con picchi ricorrenti durante le festività e alla fine dell'anno, periodi in cui le aziende riducono le attività operative e i livelli di sicurezza sono più vulnerabili.

In aggiunta, l'analisi delle vulnerabilità (CVE) ha messo in evidenza come i gruppi ransomware sfruttino tempestivamente falle di sicurezza critiche, spesso prima che le organizzazioni possano applicare le necessarie patch. Questo scenario rende ancora più urgente l'adozione di soluzioni di sicurezza proattive, che permettano alle aziende di ridurre il rischio derivante da vulnerabilità non corrette, aumentando la resilienza contro gli attacchi.

Infine, è emersa una chiara correlazione tra l'aumento degli attacchi ransomware e eventi geopolitici significativi, come conflitti internazionali, tensioni politiche ed elezioni. Alcuni gruppi sembrano agire non solo per motivi economici, ma anche per obiettivi politici e ideologici. In particolare, gruppi come MosesStaff e Handala hanno concentrato le loro operazioni su paesi specifici, come Israele, perseguendo finalità che vanno oltre il semplice profitto.