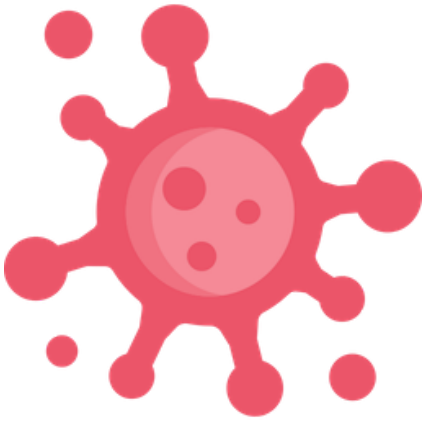


DRM / REPORT Q1 2023

Dashboard Ransomware Monitor

www.ransomfeed.it

Immagine generata da AI

INTRODUZIONE AL REPORT

Siamo lieti di presentare il **primo report quadrimestrale dell'anno 2023** sulle attività dei gruppi ransomware a livello globale. Grazie alla nostra piattaforma web di OSINT, abbiamo raccolto e analizzato una vasta quantità di dati relativi alle rivendicazioni di questi gruppi, offrendo una panoramica completa delle tendenze e dei modelli emergenti nel mondo della sicurezza informatica.

Nel corso dei primi quattro mesi dell'anno, abbiamo assistito ad un **continuo aumento delle attività ransomware**, con un numero sempre crescente di gruppi che si sono resi protagonisti di attacchi di vario

genere. Grazie ai nostri strumenti di analisi, siamo stati in grado di identificare le tattiche e le tecniche utilizzate da questi gruppi, così come le vittime più colpite e i paesi maggiormente interessati.

In questo report, esamineremo in dettaglio i dati raccolti durante il primo quadrimestre dell'anno, fornendo informazioni preziose per chiunque sia interessato alla sicurezza informatica e alla prevenzione degli attacchi ransomware. Speriamo che questo report possa contribuire a una maggiore consapevolezza dei rischi e delle minacce presenti online, e a una maggiore capacità nella protezione delle informazioni e dei sistemi di chi ci legge.

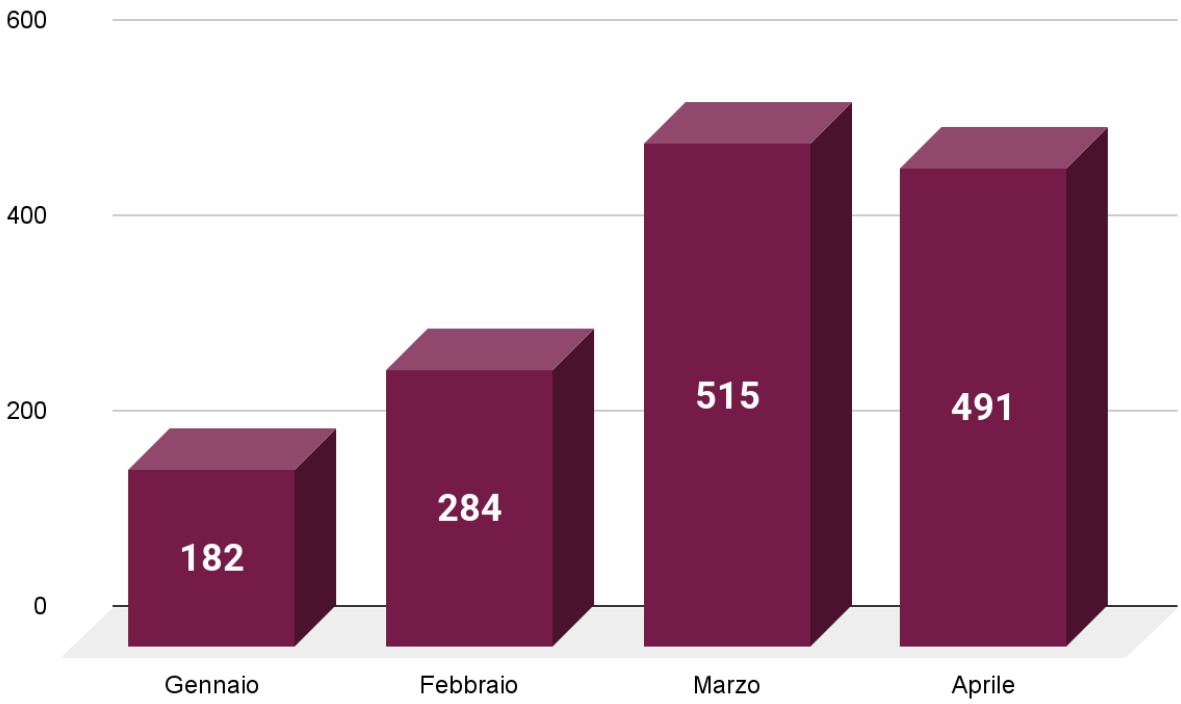
> Un codice IBAN o un numero di carta di credito possiamo sostituirli con un appuntamento in ufficio. Un dato personale rubato, è perso per sempre.
>
> Dario Fadda

Panoramica

I seguenti dati sono stati ottenuti, appunto dalla **piattaforma DRM** (www.ransomfeed.it) che effettua lo *scraping* periodico da vari siti noti del dark web utilizzando la connessione del *torsock*. Per questo rapporto, ci concentreremo sui risultati raccolti relativamente al primo quadrimestre, a livello globale, di tutti i gruppi ransomware monitorati e, vista l'appartenenza geografica del progetto DRM, con un particolare focus sull'Italia.

Per fare questo, la piattaforma ne1 1°Q 2023 ha monitorato **149** gruppi cyber criminali operanti con tecnologie ransomware, in oltre **268** server e mirrors sparsi per il Web; producendo così una raccolta di **1472** rivendicazioni di tipo ransomware identificate a livello mondo.

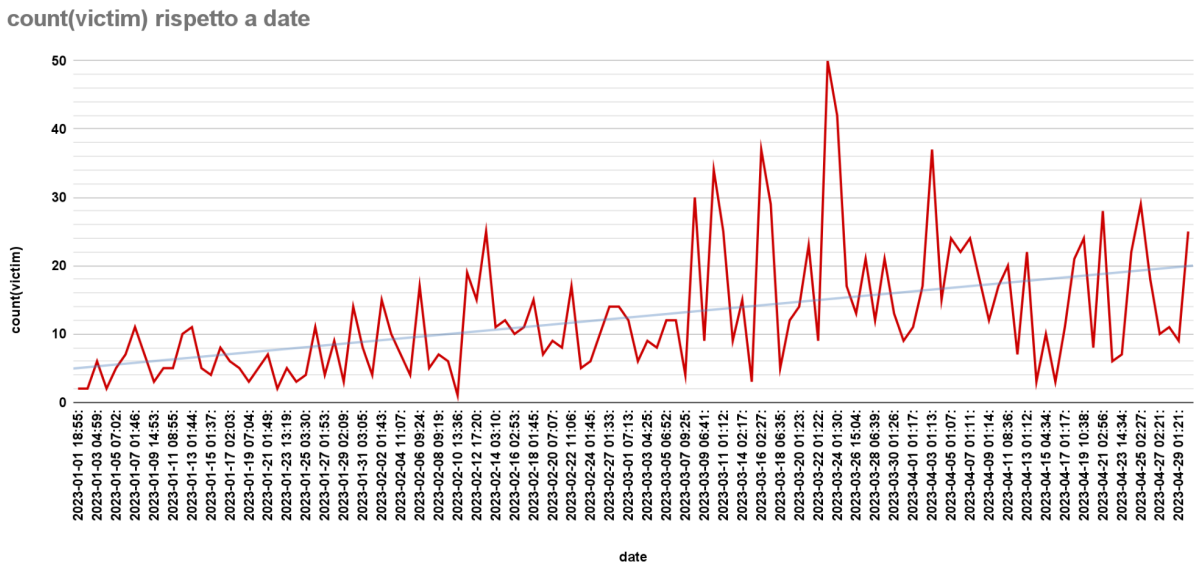
Alla luce di questa attività, è interessante rilevare come i **mesi di Marzo e Aprile** si attestino essere i più prolifici del quadrimestre con rispettivamente 515 e 491 rivendicazioni ransomware rilevate.



Attacchi suddivisi per mese - Fonte dati DRM

Mentre invece tra le giornate più attive spiccano quelle della parte centrale del quadrimestre (mese di Marzo). Il giorno più “ricco” di rivendicazioni criminali ransomware, in questo quadrimestre è stato il **23 marzo** con **50 vittime** a livello globale. Il giorno più “povero” di attacchi ransomware è stato il **10 febbraio** con una sola

rivendicazione. A completare il quadro dei primi 120 giorni dell'anno, sono presenti due giornate senza alcuna rivendicazione, il 25 Febbraio e il 12 Marzo.

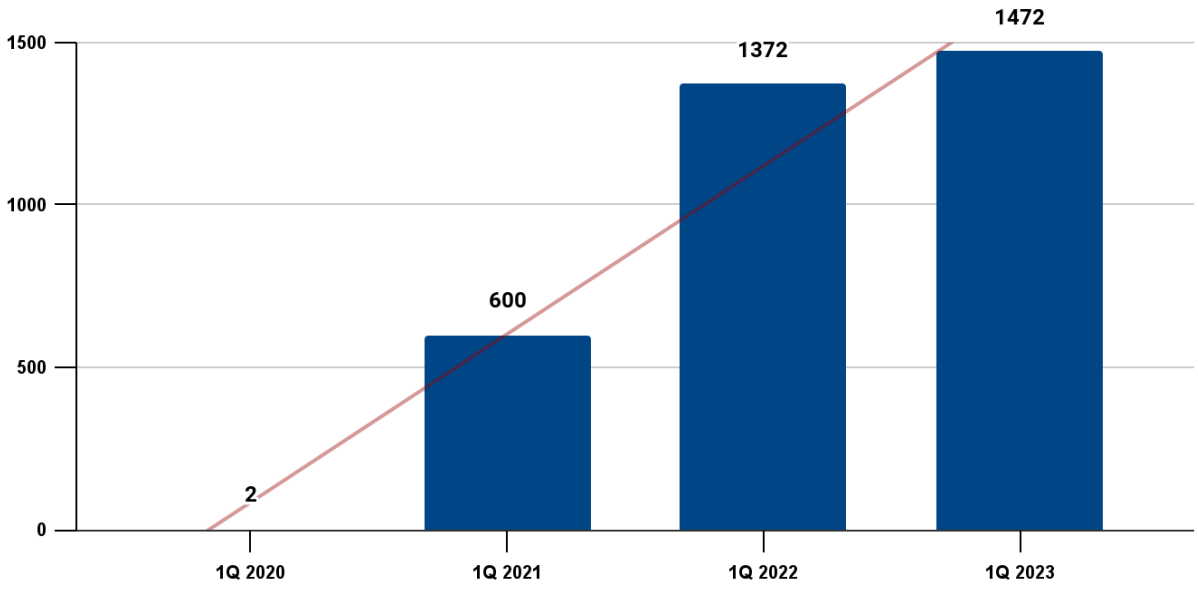


Nella linea di fondo si evidenzia il trend complessivo medio (fonte dati DRM)

Il dato di questo trend si traduce con una media a livello mondiale di **12 attacchi di tipo ransomware rivendicati ogni giorno**.

Quadrimestri a confronto

Nell'ottica di inquadrare in maniera puntuale i dati appena esposti nella Panoramica, abbiamo raffrontato il dato con alcuni primi quadrimestri del passato. Ricordando infatti che la piattaforma DRM è stata inizialmente alimentata con i dati pregressi fino al 12 gennaio 2020, siamo tornati indietro nel tempo, interrogando così il 1°Q degli ultimi tre anni.

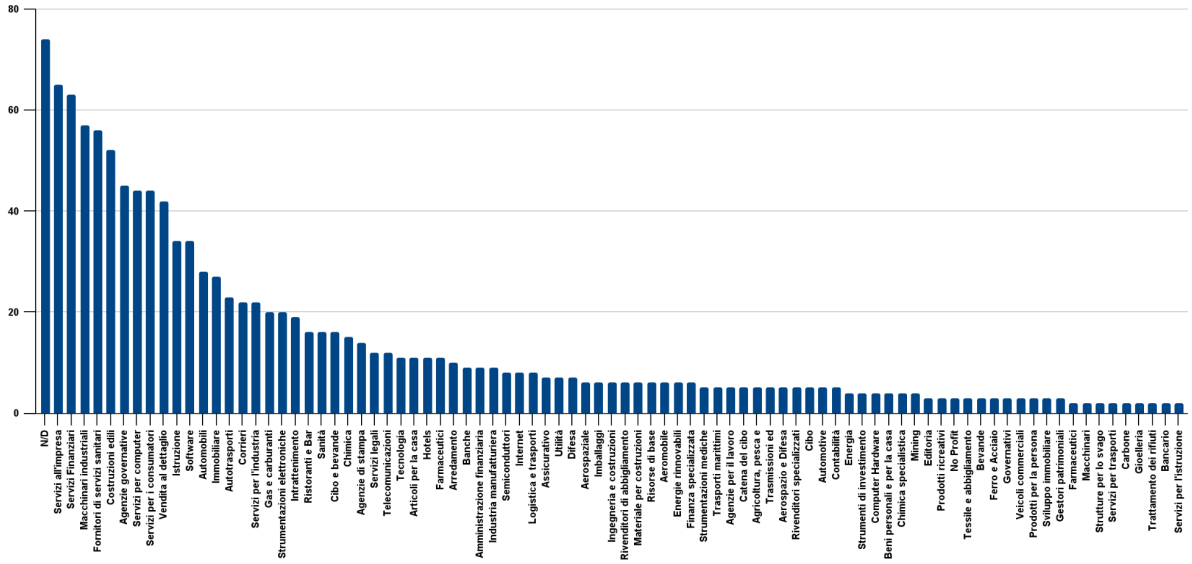


Come si può vedere anche dal grafico che riporta i dati, **il trend è in crescita** e ancora non si registra una diminuzione degli attacchi ransomware. In questo quadro temporale infatti anche il 2023 attesta un aumento rispetto al Q1 2022 di quasi **8%**. È invece da considerarsi positivo il **tasso di crescita** rispetto ai quadrimestri degli anni precedenti, che sembra avviare un percorso di diminuzione. Il dato del Q1 2022 infatti registrò una variazione rispetto allo stesso periodo dell'anno precedente (2021) di ben 129 punti percentuali.

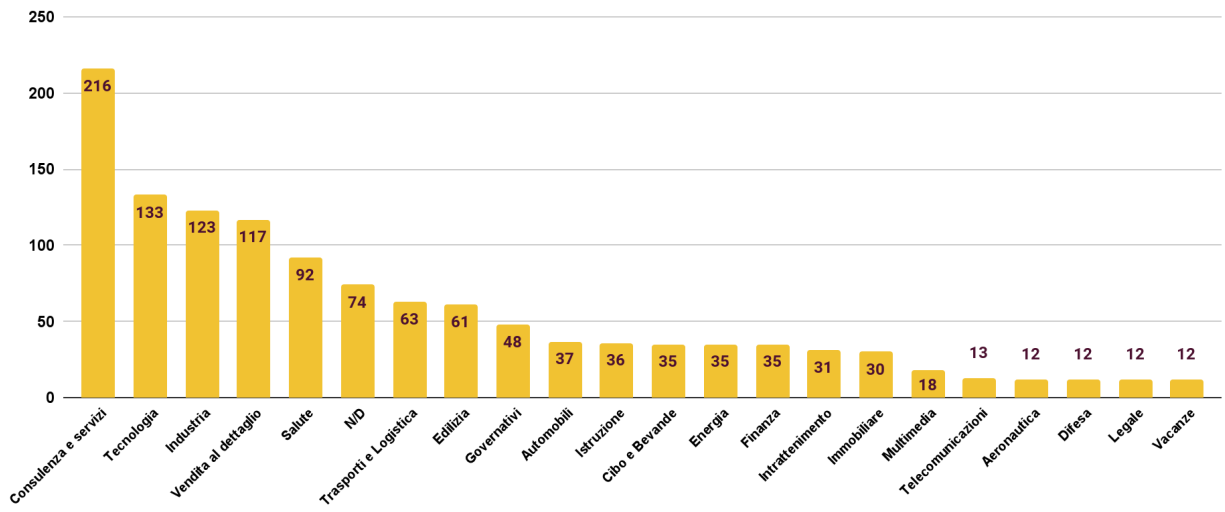
DISTRIBUZIONE DEL RANSOMWARE NEI SETTORI LAVORATIVI

- - - - 2

Dall’analisi dei dati delle vittime coinvolte, si può concludere che a livello mondiale il settore lavorativo di riferimento più colpito è stato quello dei **servizi all’impresa.** Il risultato del settore servizi è confermato dall’aggregazione dei dati in maniera specifica, con una classificazione dettagliata di 87 categorie economiche distinte.



Verificando anche con una differente aggregazione dei dati, generata dalla distinzione delle vittime in 22 macro aree settoriali, il settore dei **Servizi e consulenza**, è sempre il più colpito del quadrimestre **con il 17,3% degli attacchi**.



Gli attacchi per le 22 macro categorie lavorative (fonte dati DRM)

Il podio dei settori lavorativi viene completato dal secondo posto con quasi l'11% per **Tecnologia** e **Industria** seguiti da **Vendita al dettaglio** sotto il 10% e **Salute al 7,4%**.

Macro settori	% 1Q-2023		
Consulenza e servizi	17,3	Cibo e Bevande	2,8
Tecnologia	10,7	Energia	2,8
Industria	9,9	Finanza	2,8
Vendita al dettaglio	9,4	Intrattenimento	2,5
Salute	7,4	Immobiliare	2,4
N/D	5,9	Multimedia	1,4
Trasporti e Logistica	5,1	Telecomunicazioni	1,0
Edilizia	4,9	Aeronautica	1,0
Governativi	3,9	Difesa	1,0
Automobili	3,0	Legale	1,0
Istruzione	2,9	Vacanze	1,0

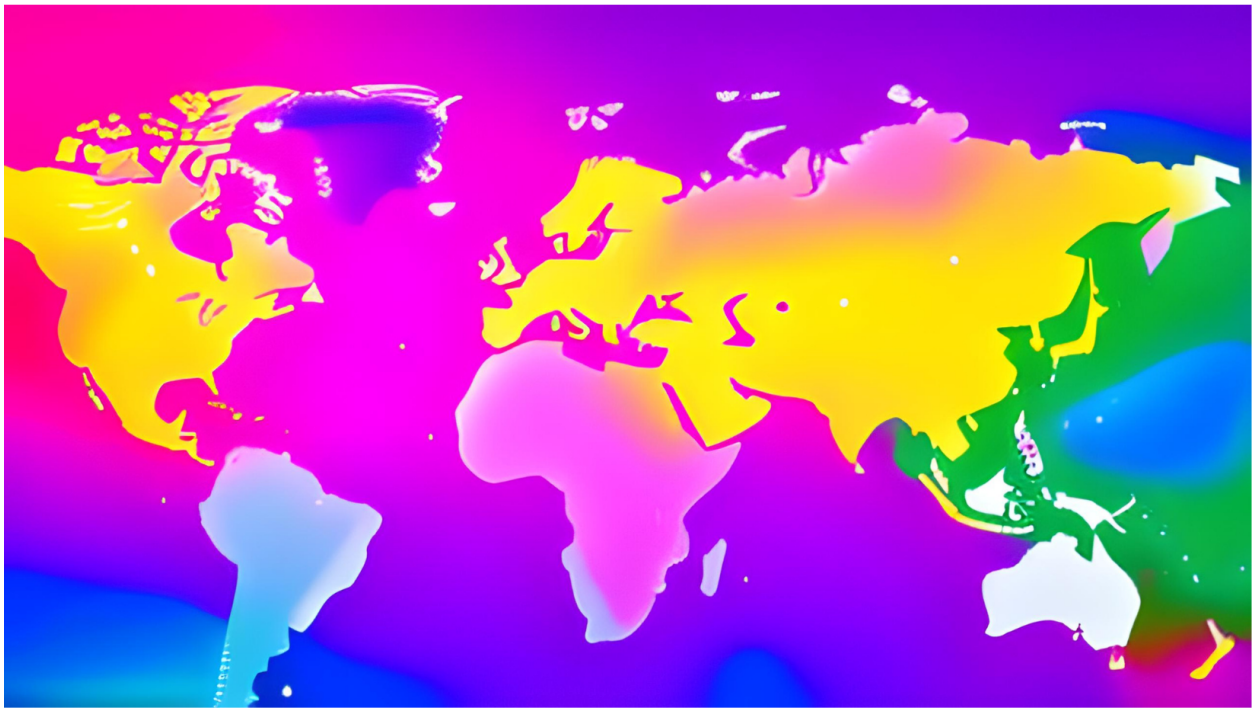


Immagine generata da AI

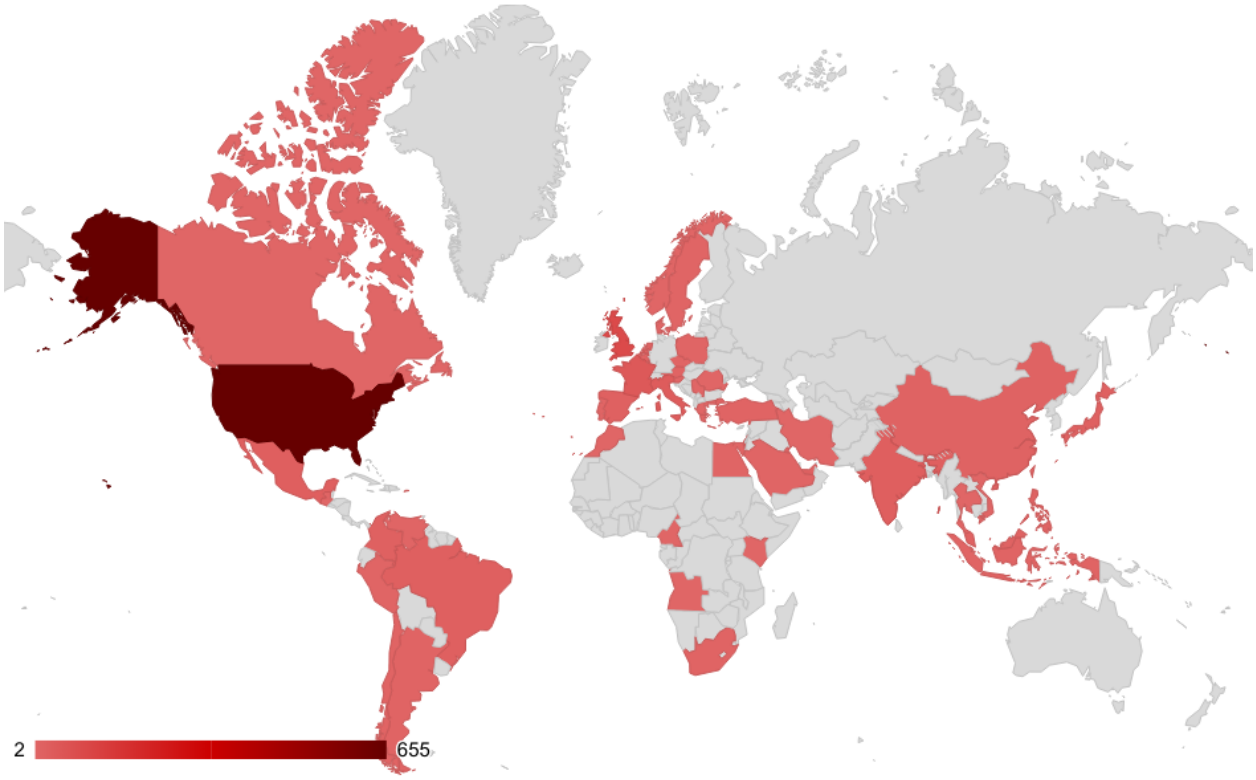
DISTRIBUZIONE DEL RANSOMWARE NEL MONDO

– – – – 3

I risultati della piattaforma DRM hanno permesso di investigare la geografia delle vittime rivendicate nel corso del quadrimestre.

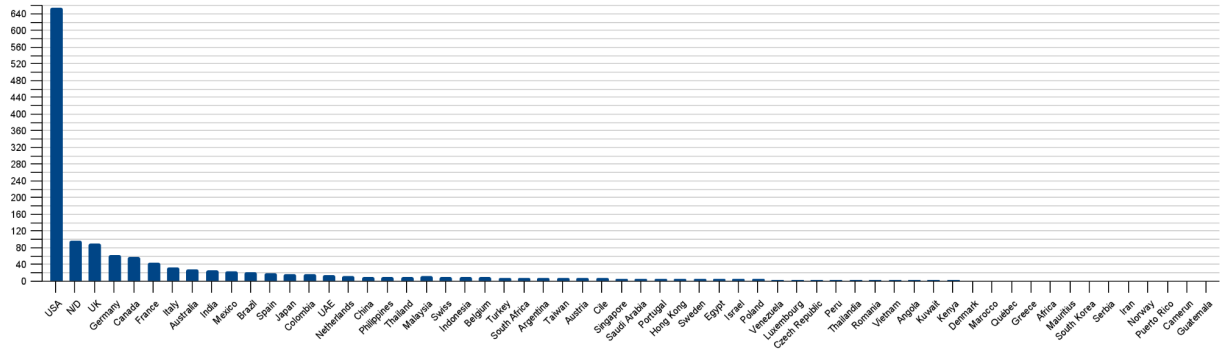
Da una prima estrazione massiva dei dati è possibile notare come **la fascia nord-occidentale del mondo** sia la più gravemente impattata dai gruppi criminali informatici.

Nella figura che segue è possibile evidenziare gli effetti di una rappresentazione su mappa di questo risultato.



Nelle gradazioni di rosso gli Stati con vittime (fonte dati DRM)

Una traduzione puntuale dell'interezza dei dati estratti, consente di confermare gli **USA come primo paese del mondo per numero di vittime** ransomware nel Q1-23, con il 44,5% del totale. I Paesi coinvolti sono stati complessivamente 92 (a fine sezione la tabella con tutte le distribuzioni rilevate).



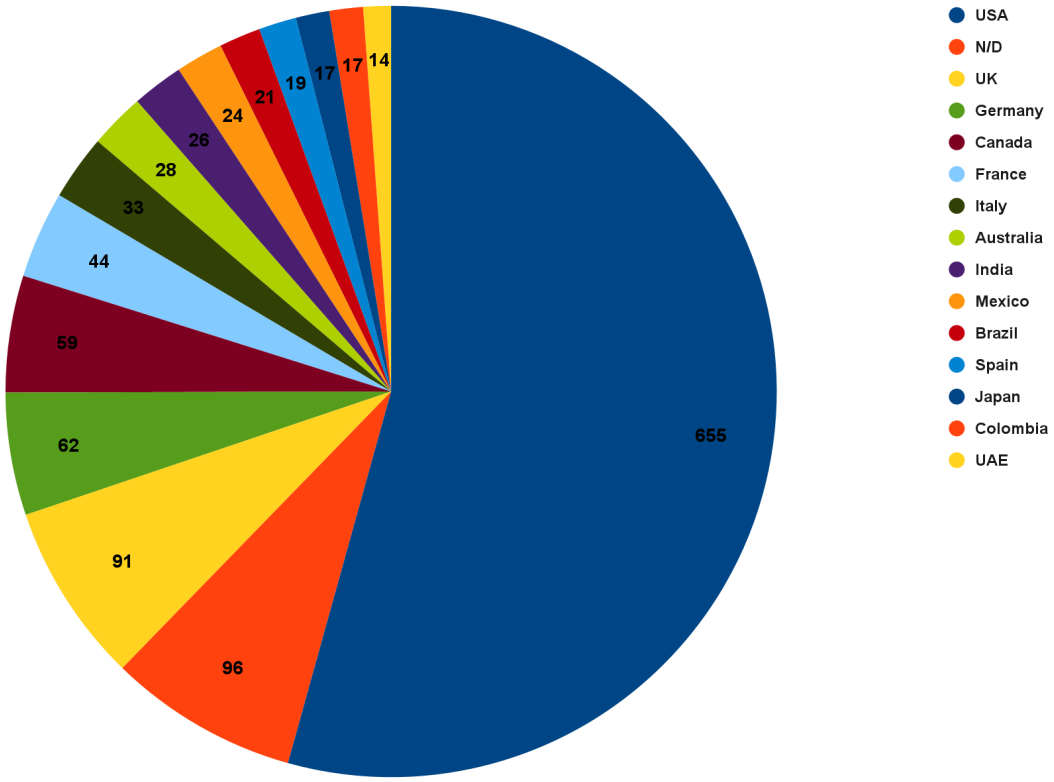
Considerato che circa il 6,5% degli attacchi analizzati non sono puntualmente localizzabili geograficamente (per via di dati mancanti o non esaustivi), gli Stati Uniti sono seguiti da Regno Unito (6,2%), Germania (4,2%) e Canada (4%).

L'Italia si trova al sesto posto con il 2,2% di vittime subito dopo la Francia (3%); a questo proposito si fa notare che una delle prossime sezioni di questo report è dedicata proprio al "Focus sull'Italia", con **analisi dei dati specialistica**.

Paese	%						
USA	44,5	Turkey	0,5	Kenya	0,2	Palestine	0,1
N/D	6,5	South Africa	0,5	Denmark	0,1	Dominican Republic	0,1
UK	6,2	Argentina	0,5	Marocco	0,1	Barbados	0,1
Germany	4,2	Taiwan	0,5	Québec	0,1	Hungary	0,1
Canada	4,0	Austria	0,5	Greece	0,1	Pakistan	0,1
France	3,0	Cile	0,5	Africa	0,1	Algeria	0,1
Italy	2,2	Singapore	0,4	Mauritius	0,1	Slovakia	0,1
Australia	1,9	Saudi Arabia	0,4	South Korea	0,1	Saint Kitts and Nevis	0,1
India	1,8	Portugal	0,4	Serbia	0,1	Panama	0,1
Mexico	1,6	Hong Kong	0,4	Iran	0,1	Scandinavia	0,1
Brazil	1,4	Sweden	0,3	Norway	0,1	Tasmania	0,1
Spain	1,3	Egypt	0,3	Puerto Rico	0,1	Estonia	0,1
Japan	1,2	Israel	0,3	Camerun	0,1	Finland	0,1
Colombia	1,2	Poland	0,3	Guatemala	0,1	Korea	0,1
UAE	1,0	Venezuela	0,3	Slovenia	0,1	Bangladesh	0,1
Netherlands	0,8	Luxembourg	0,3	Maldives	0,1	Cyprus	0,1
China	0,7	Czech Republic	0,3	Republic of Trinidad and Tobago	0,1	Macedonia	0,1
Philippines	0,7	Peru	0,3	Ecuador	0,1	Nigeria	0,1
Thailand	0,7	Thailandia	0,2	Albania	0,1	Oman	0,1
Malaysia	0,8	Romania	0,2	Jordan	0,1	Croazia	0,1
Swiss	0,6	Vietnam	0,2	Uruguay	0,1		
Indonesia	0,6	Angola	0,2	Ireland	0,1		
Belgium	0,6	Kuwait	0,2	Tonga	0,1		

I TOP 15

Ancora una volta, aggreghiamo i dati per poterli visualizzare escludendo i Paesi sotto l'1% di vittime ransomware e ne rappresentiamo il grafico per i primi 15 a livello globale, ciascuno con il numero di rivendicazioni registrate.



Top 15 per numero di vittime (fonte dati DRM)

Da questo grafico risulta maggiormente visibile il **divario tra USA e resto del mondo**, ma viene rispettata la stessa indicizzazione della classifica generale con **UK, Germania e Canada tra le prime posizioni**.

NUOVI GRUPPI CRIMINALI

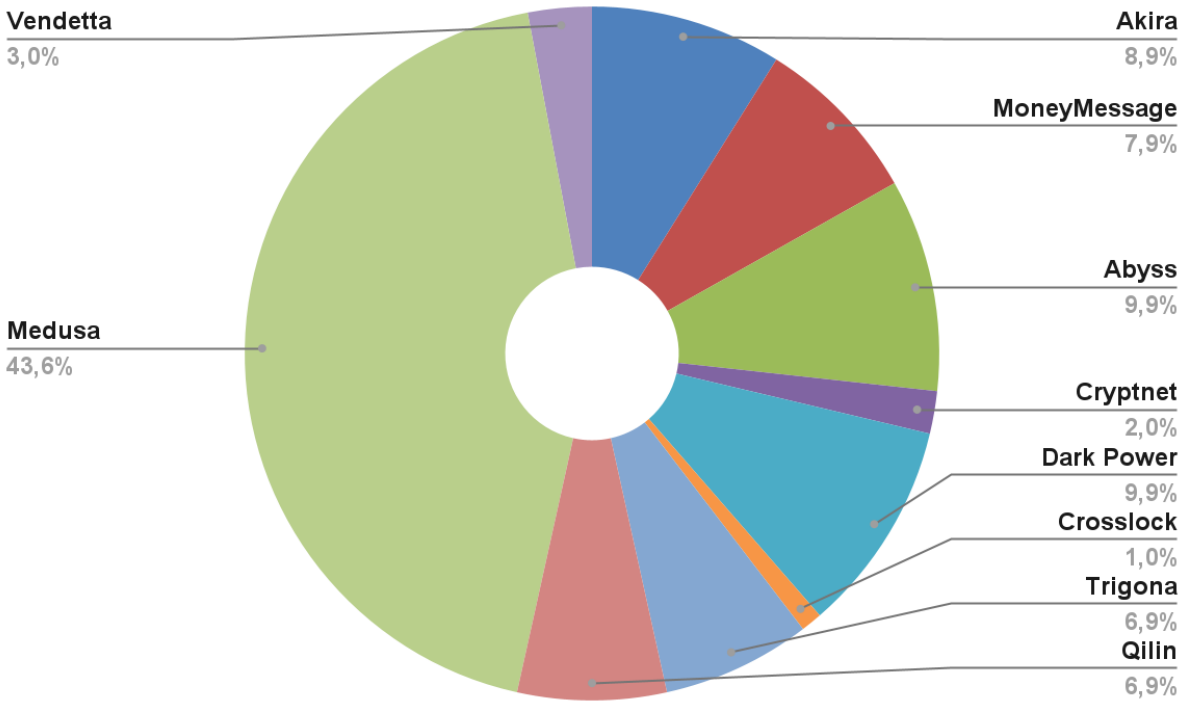
– – – – 4

Come è noto la scena del crimine informatico, anche nel caso del settore malware (in questo caso specifico analizziamo i ransomware), vedono di frequente il crescere della forza lavoro sul campo.

Il Q1-23 non è escluso e ha visto la comparsa di **11 nuovi gruppi** che insieme hanno rivendicato **101 attacchi informatici** in tutto il mondo. Poco meno di un attacco al giorno, solamente da nuovi gruppi che hanno appena iniziato le proprie operazioni criminali.

NUOVI AGGIUNTI	
Akira	9
MoneyMessage	8
Abyss	10
Cryptnet	2
Dark Power	10
Crosslock	1
Trigona	7
Qilin	7
Medusa	44
Vendetta	3
Nevada	0

La tabella sopra riportata evidenzia i gruppi che la piattaforma DRM ha aggiunto al monitoraggio nell'arco dei 120 giorni del primo quadrimestre, perché resi noti proprio nel medesimo periodo.



Riportando i dati in termini percentuali, possiamo facilmente capire quali, nel Q1-23 sono state le nuove cyber gang più attive, con **Medusa che supera il 43%**.

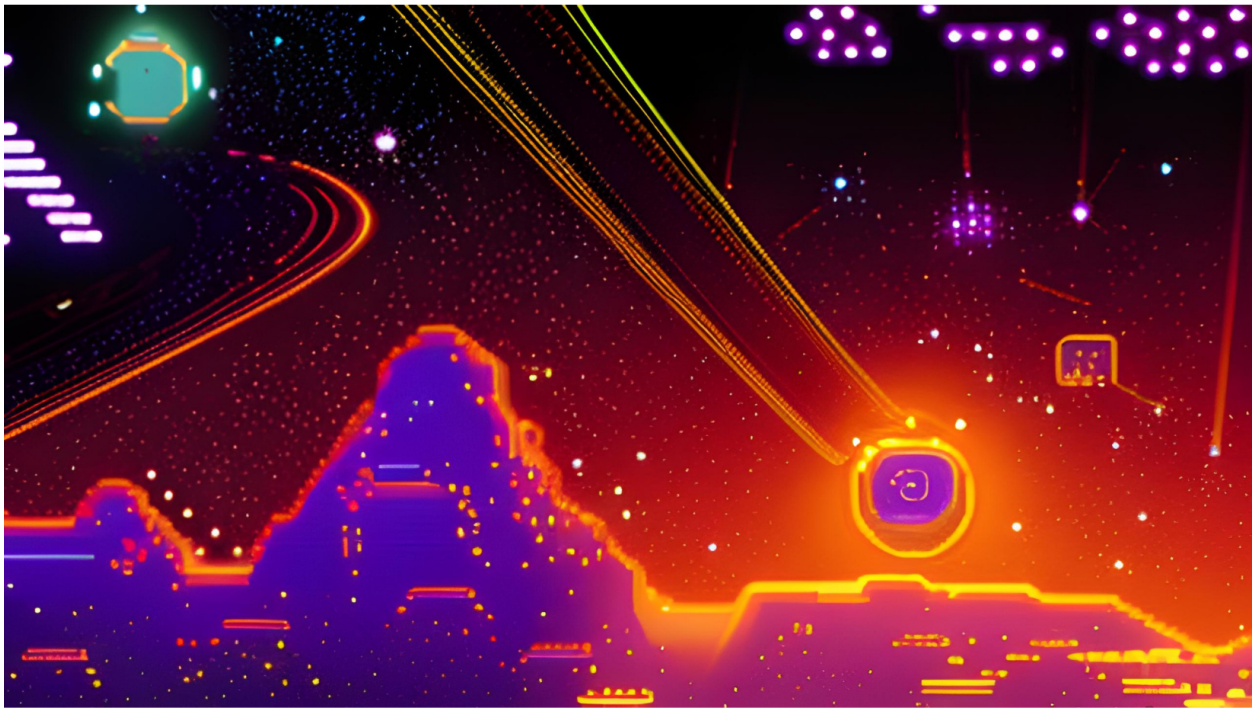


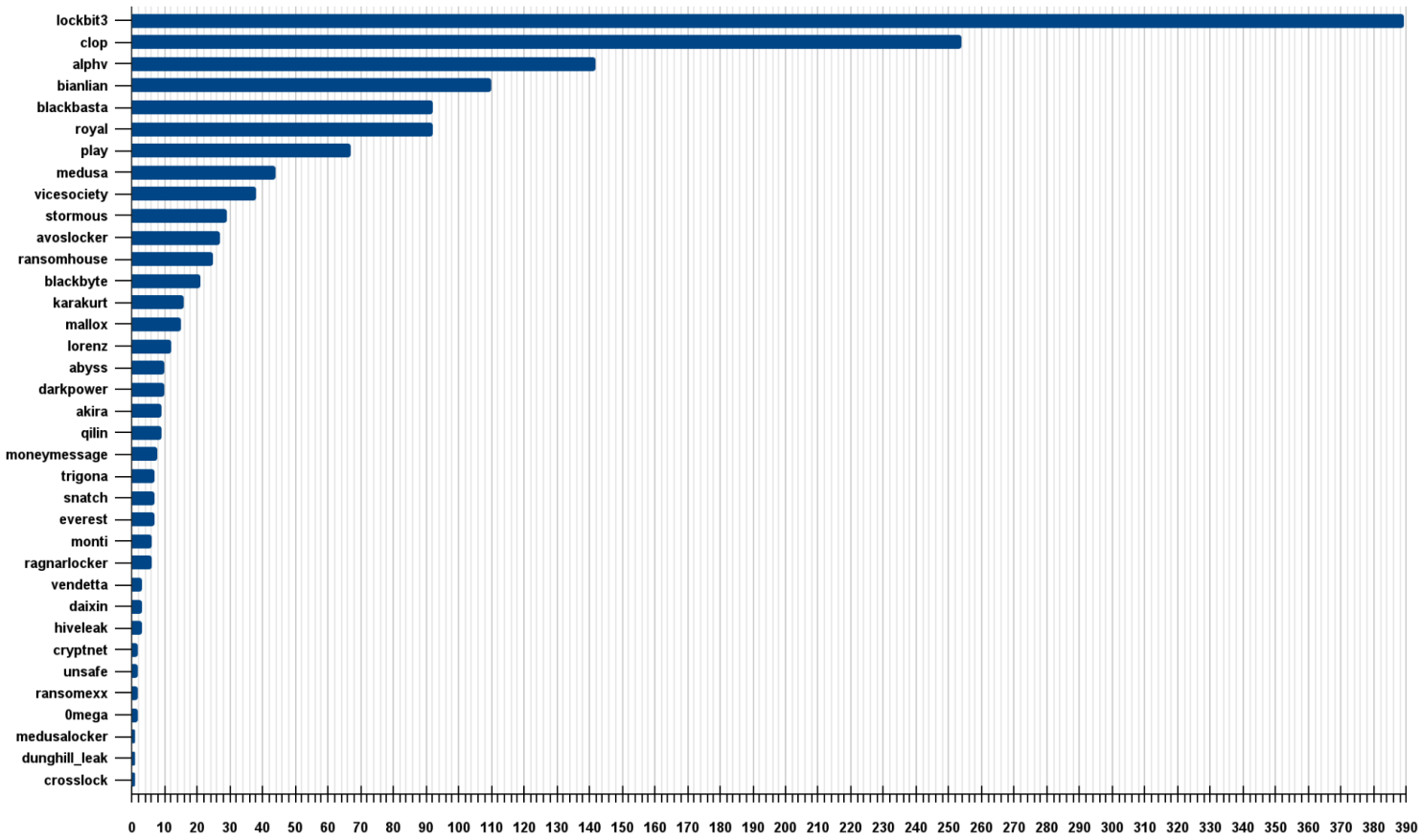
Immagine generata da AI

LE ATTIVITÀ GLOBALI DEI GRUPPI RANSOMWARE

Uno dei cluster analizzati per questo report contiene dei dati relativi ai singoli gruppi criminali. Tra tutti i gruppi che costantemente vengono monitorati, la piattaforma ha rilevato attività nel quadrimestre per 36 di questi. Gli altri sono risultati inattivi.

Le attività di questi gruppi hanno prodotto il totale dei dati che stiamo analizzando nelle pagine di questo report e hanno visto una leadership assoluta di tre gruppi estremamente attivi, capaci da soli, di dividersi il 53% degli attacchi. Il trio è guidato dal gruppo criminale **LockBit che da solo conta il 26,4%** degli attacchi; seguito da **Clop** e **ALPHV/BlackCat** rispettivamente con il 17,3% e 9,6%.

Un dettaglio puntuale di tutte le 36 cyber gang attive è offerto dal grafico seguente, il cui valore di riferimento è attribuito al numero di vittime rivendicate. Possiamo così monitorare anche l'attività, a livello mondiale, dei gruppi per ora meno attivi.



A questo proposito si fa notare che i dati di LockBit qui riportati, sono da attribuire all'operazione lockbit3 (le precedenti sono infatti dismesse e non più attive) e che questo nuovo rebranding è stato portato a termine di recente, con un cambio avvenuto nel mese di Giugno 2022.

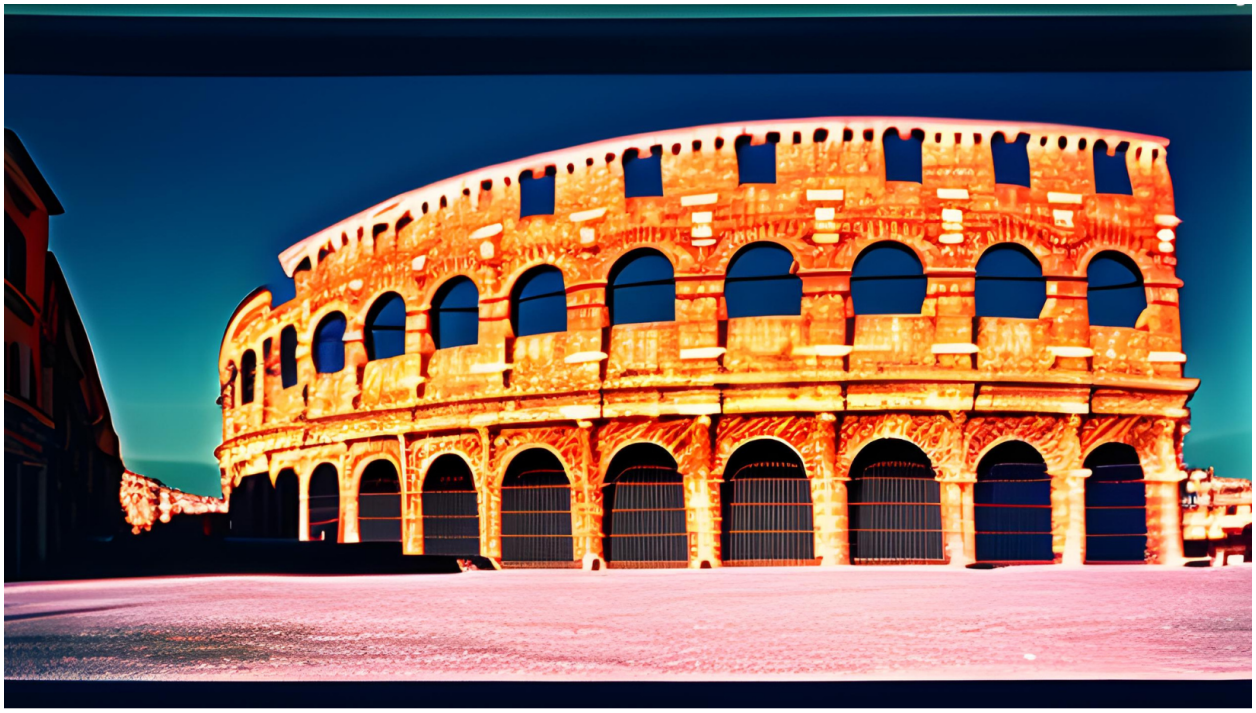


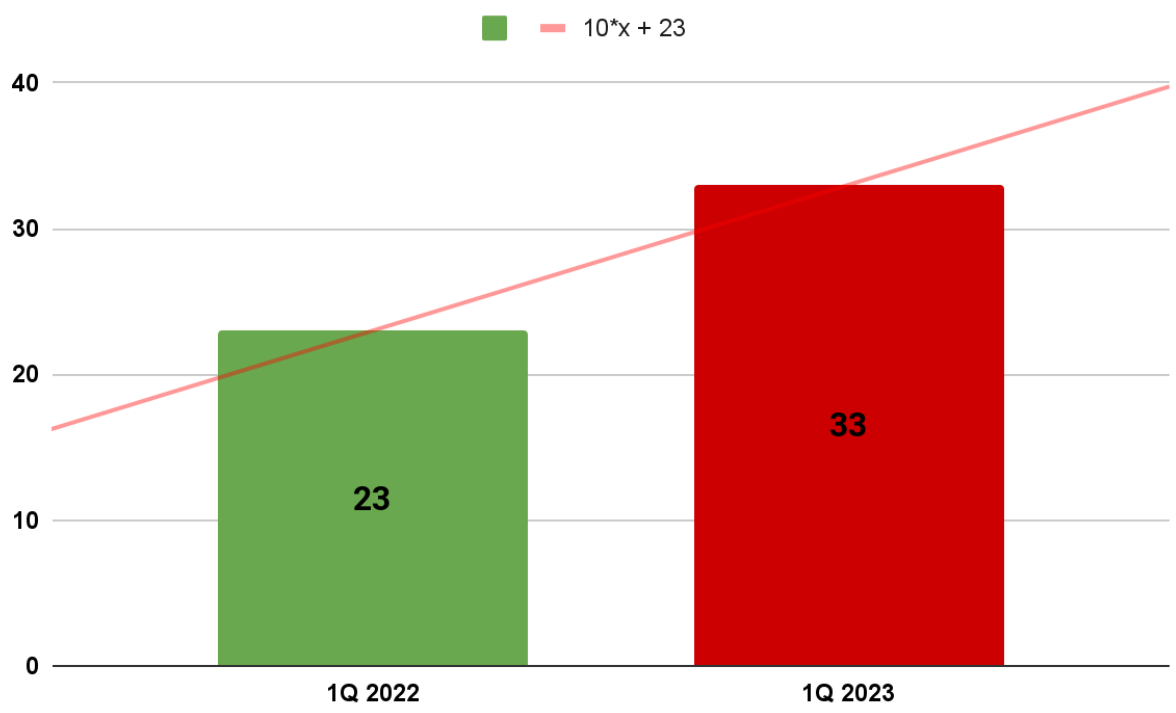
Immagine generata da AI

FOCUS ITALIA Q1-23

Come premesso nell'Introduzione di questo report, essendo la piattaforma DRM (Dashboard Ransomware Monitor) un progetto italiano, sentiamo doveroso voler dedicare una sezione di questo report all'analisi dei dati relativi all'Italia.

Questa sezione dunque, riporta tutte le analisi già precedentemente trattate a livello globale nelle sezioni precedenti, ma con le *query* specifiche per l'Italia.

Il primo dato che sicuramente emerge è il numero degli **attacchi ransomware che hanno coinvolto l'Italia nel Q1-23, sono stati 33**. Circa uno ogni 84 ore.



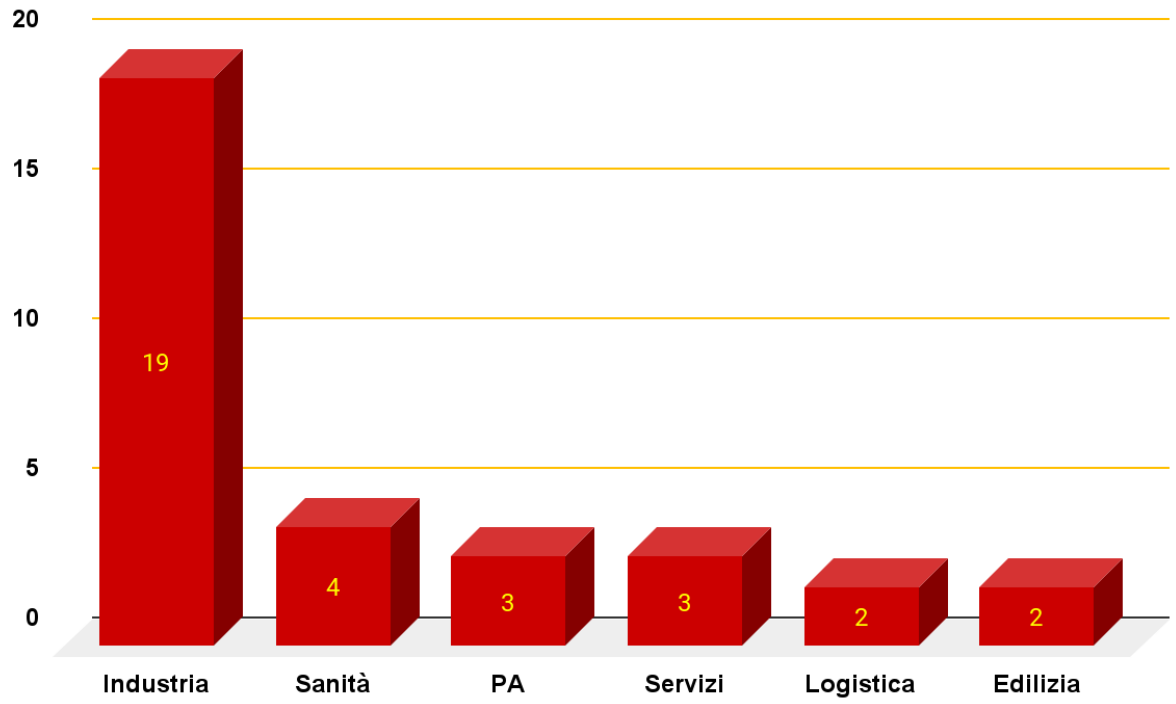
Questo dato rispecchia perfettamente il trend globale, in costante crescita rispetto allo stesso periodo dell'anno precedente. Tuttavia il **tasso di crescita, in Italia è del 44%** rispetto al 2022.

Gli attacchi per settore economico

La categoria maggiormente colpita da attacchi di tipo ransomware, nel Q1-23 si evidenzia l'**Industria**, in maniera generica (tra queste, quella farmaceutica, meccanica, metallurgica ed elettronica), con 19 attacchi ransomware rivendicati nel periodo.

Oltre il **57% occupato dall'industria**, segue il **settore Sanitario** e quello della **Pubblica Amministrazione**, i cui numeri tuttavia scendono e si distanziano dal settore primario, tra 12% e 9%.

Una ripartizione dei dati puntuale, di tutti i settori lavorativi viene riportata nel grafico qui di seguito.



In termini percentuali, possiamo leggere questi dati anche con la tabella qui sotto, che ci aiuta in fase di analisi ad interpretarli per ogni categoria, rispetto al totale degli attacchi.

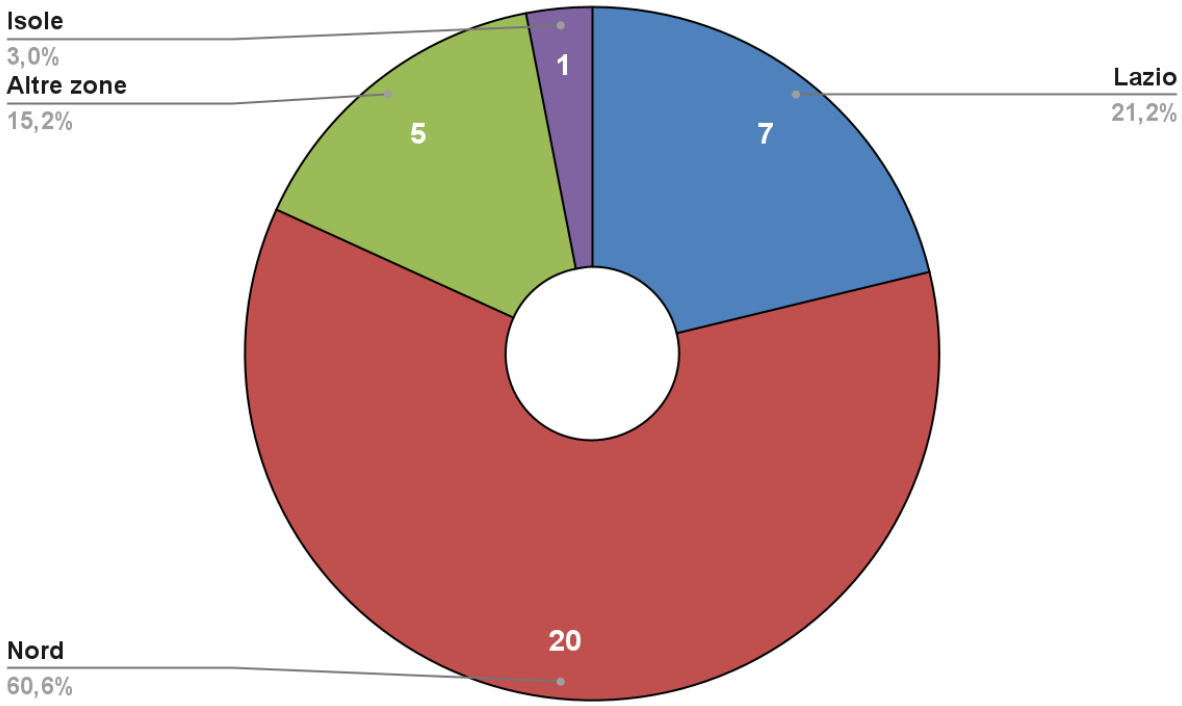
Settori aggregati	%
Industria	57,6
Sanità	12,1
PA	9,1
Servizi	9,1
Logistica	6,1
Edilizia	6,1

La distribuzione del ransomware nel territorio

Con i dati sulla localizzazione delle vittime operata dalla piattaforma DRM siamo stati in grado di disegnare una mappa per definire la distribuzione geografica del ransomware in Italia, per il Q1-23. La mappa seguente è anche consultabile online, con le funzione interattive, al seguente indirizzo: https://www.google.com/maps/d/u/1/edit?mid=1qDLdY_C-QX8XwhS5YI1VRJ0nARXQ2PI&usp=sharing

Oltre il **60%** delle rivendicazioni è afferente ad organizzazioni ed enti del **nord Italia**.

Se suddividiamo la mappa in macro aree geografiche otteniamo una rappresentazione sinottica come da grafico seguente.

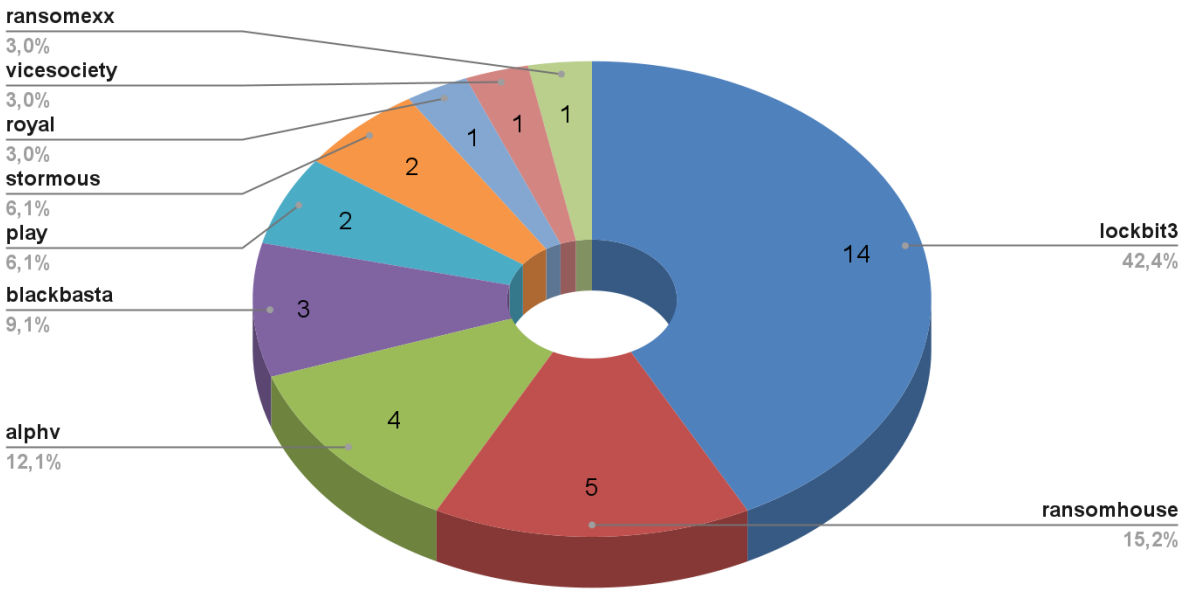


I gruppi criminali più attivi

Il dato mondiale si rispecchia anche per quanto riguarda l'analisi delle cyber gang che hanno condotto/rivendicato gli attacchi sul territorio nazionale.

In effetti **LockBit** si attesta essere **il gruppo più attivo anche in Italia**, per il quadrimestre con il 42,4% degli attacchi.

Seguono, con importante distanza, **Ransomhouse** e **ALPHV/BlackCat**, che insieme si spartiscono quasi in maniera omogenea il 27,3%.



Dal grafico viene evidenziata la totalità degli attacchi contro vittime italiane, riportando le percentuali di ogni gruppo e con il dato all'interno, il numero di vittime rivendicate.

CONCLUSIONE

I dati che questo report ha portato alla luce e analizzato evidenziano come il ransomware, in tutto il mondo Italia compresa, non sia una minaccia da dimenticare. Sta seguendo un trend sempre crescente rispetto allo stesso periodo degli anni precedenti, un tasso di crescita dell'8% che genera tuttavia un comportamento ottimistico se rapportato al tasso dello stesso periodo di due anni prima (che era del 129%).

L'Italia è il sesto Paese al mondo per numero di attacchi ransomware, mentre gli Stati Uniti occupano la prima posizione con il 44,5% degli attacchi localizzati all'interno della propria area geografica.

LockBit (operazione 3) si afferma come il gruppo criminale più prolifico del mondo, sia appunto a livello globale che italiano.

In sintesi, l'analisi dei dati sulle operazioni dei gruppi ransomware evidenzia una tendenza all'aumento del numero di attacchi e alla sofisticazione delle tecniche utilizzate. La diffusione di questi attacchi rappresenta una minaccia crescente per le organizzazioni di ogni settore e dimensione. La protezione contro questi attacchi richiede una combinazione di tecnologie di sicurezza avanzate, prassi di sicurezza solide e formazione dei dipendenti. Inoltre, la cooperazione tra organizzazioni e governi a livello nazionale e internazionale è essenziale per mitigare l'impatto dei ransomware sulle comunità globali.

Dashboard Ransomware Monitor

www.ransomfeed.it