DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

REPORT Q2 2023

DASHBOARD RANSOMWARE MONITOR

RANSOMFEED | RANSOMFEED.IT

DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

INDICE

DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

INTRODUZIONE AL REPORT

Questo report si propone di **fornire un approfondimento dettagliato** sul panorama delle **minacce ransomware** nel periodo compreso tra Maggio e Agosto 2023 (secondo quadrimestre), con un **particolare focus** sulle attività di monitoraggio condotte dalla piattaforma **OSINT DRM**.

Durante questo periodo di tempo sono stati **monitorati 165 gruppi criminali** operanti in tutto il mondo, con un costante **tracciamento di 300 server** impiegati per condurre attività di ransomware.

I dati raccolti hanno evidenziato un totale di **1736 rivendicazioni ransomware**, di cui **53 registrate in Italia**.

Il report esamina attentamente la **localizzazione geografica** di tali attacchi, nonché il settore lavorativo maggiormente interessato.

Inoltre, viene dedicata un'attenzione speciale agli attacchi ransomware che hanno colpito **l'Italia**, al fine di comprendere le sfide specifiche che il paese ha affrontato durante questo periodo critico in materia di sicurezza informatica.

DRM
AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

> Ciò che proteggiamo oggi nel cyberspazio è ciò che ci preserverà domani nella nostra vita digitale.
>
> *Dario Fadda*

PANORAMICA

Tutti i dati, come da nostra prassi, sono stati ottenuti tramite la primaria **attività della piattaforma DRM Ransomfeed** di scraping periodico da una selezione di siti noti nel dark web.

Per questo rapporto ci concentreremo sui risultati raccolti relativamente al **secondo quadrimestre dell'anno**: prima a livello globale, con tutti i gruppi ransomware monitorati e, successivamente, con un particolare **focus sull'Italia**.

La piattaforma nel Q2 2023 ha **monitorato 165 gruppi cyber criminali** operanti con tecnologie ransomware in oltre **300 server e mirrors**, totalizzando così una definizione di **1736 rivendicazioni** di tipo ransomware identificate a livello mondiale.

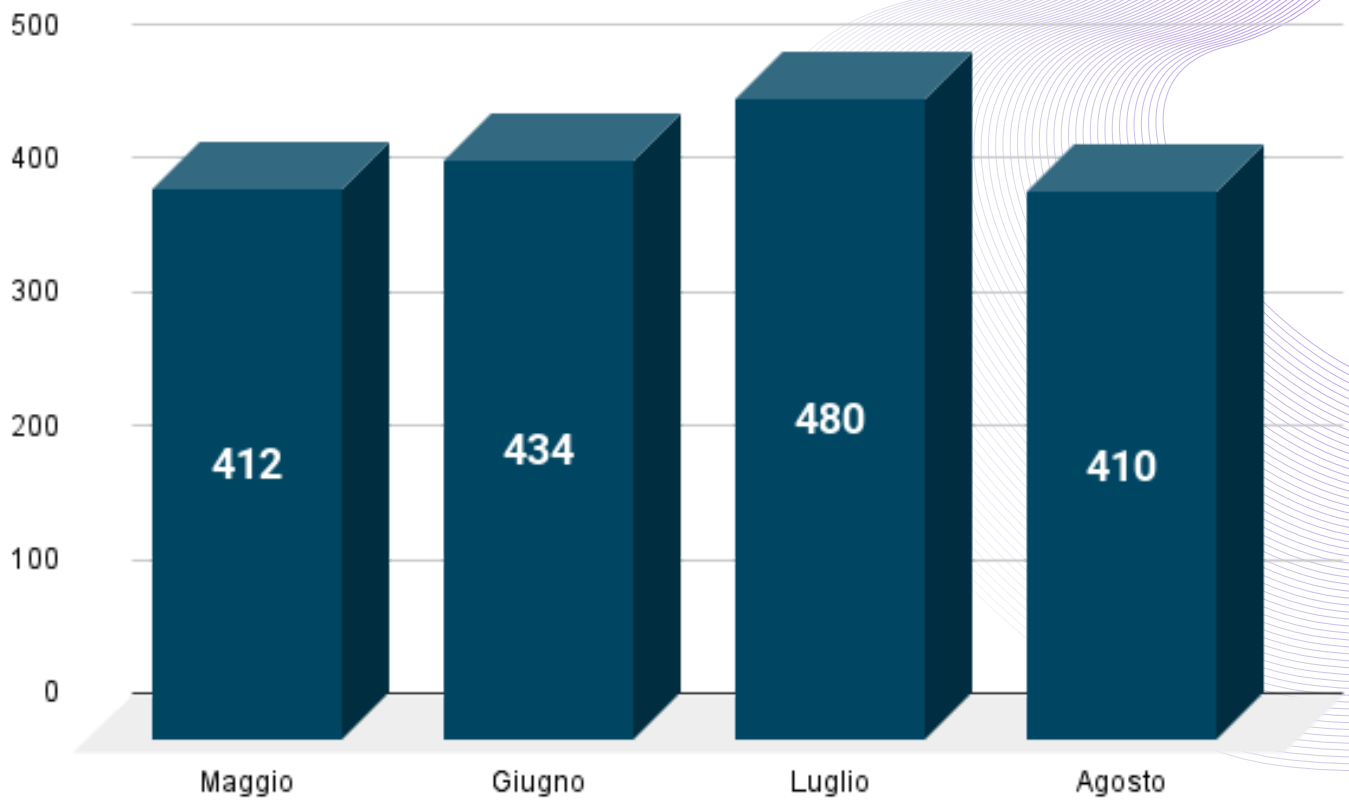
I mesi di **Maggio**, **Giugno**, **Luglio** ed **Agosto** hanno tutti presentato sfide uniche nel campo della cybersecurity.

Il mese di **Maggio** ha inaugurato il quadrimestre **con 412 attacchi**, seguito da **Giugno** con 434, **Luglio** con 480 e **Agosto** con 410.

Tuttavia, è il **dettaglio dei giorni** che rivela un quadro ancor più allarmante.

DRM
AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

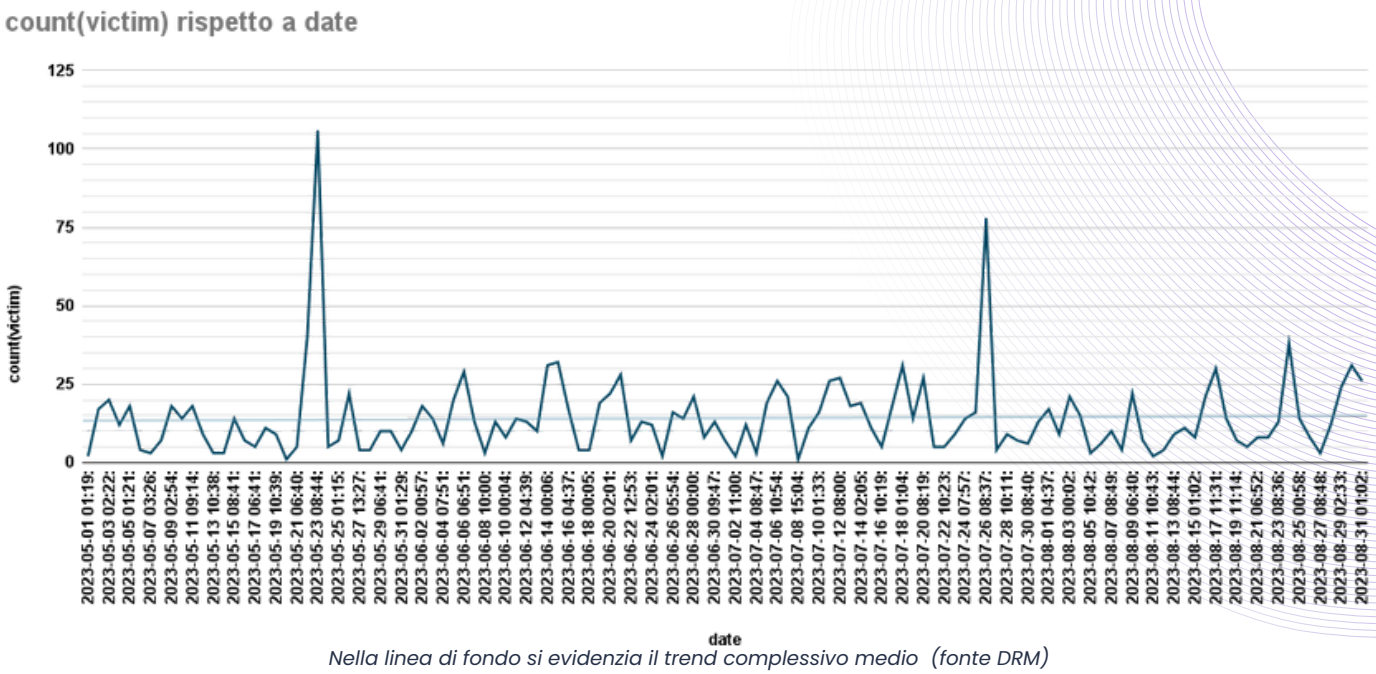


attacchi suddivisi per mese (fonte DRM)

Il **23 Maggio** è stato il punto culminante con **106 attacchi ransomware** rivendicati in un solo giorno, mettendo in luce la determinazione degli attaccanti a sfruttare le vulnerabilità digitali.

Al contrario, l'**8 Luglio** ha segnato il giorno meno rilevante del quadrimestre, con solamente una rivendicazione.

La media giornaliera di attacchi nel corso del quadrimestre **supera i 14**, un dato che richiede una seria riflessione in merito alle misure di sicurezza adottate dalle organizzazioni.

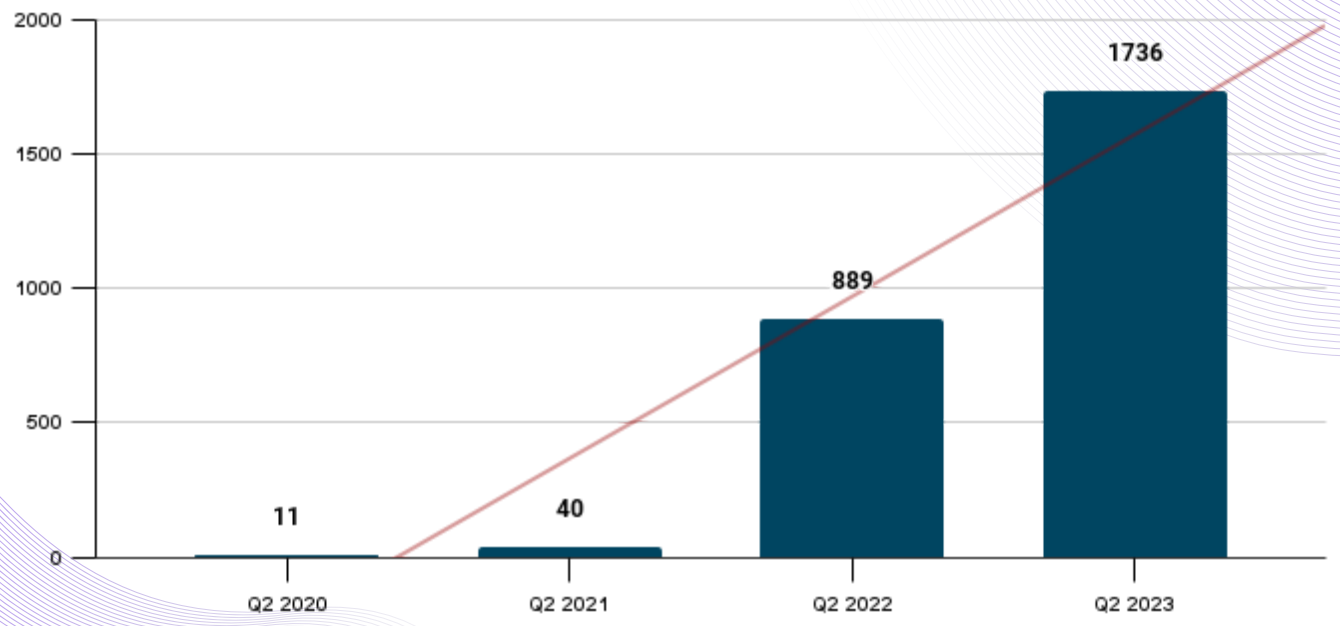


Nella linea di fondo si evidenzia il trend complessivo medio (fonte DRM)

• QUADRIMESTRI A CONFRONTO

Al fine di inquadrare in maniera puntuale i dati appena esposti nella **Panoramica**, abbiamo **confrontato il dato con alcuni segmenti del passato**.

Ricordiamo che la piattaforma DRM è stata **inizialmente alimentata con i dati pregressi fino al 12 Gennaio 2020:** ci è stato quindi possibile tornare indietro nel tempo, raffrontando il Q2 degli ultimi tre anni.



Si evince come **il trend sia in crescita** e ancora **non si registri** una diminuzione degli attacchi. In questo quadro temporale, infatti, anche il 2023 **conferma un aumento** rispetto al Q2 2022 di **oltre il 51%**.

Per quanto riguarda l'elaborazione e la presentazione dei dati del quadrimestre in oggetto, è doveroso informare che, nel corso di questi mesi, abbiamo introdotto un **sistema di gestione dei "duplicati"**. Questa caratteristica è stata **creata ed affinata internamente**, per filtrare e correggere eventuali duplicati che alcune cyber gangs generano nella pubblicazione delle vittime; ora la piattaforma presenta dei dati purificati di tutte queste "finte" rivendicazioni.

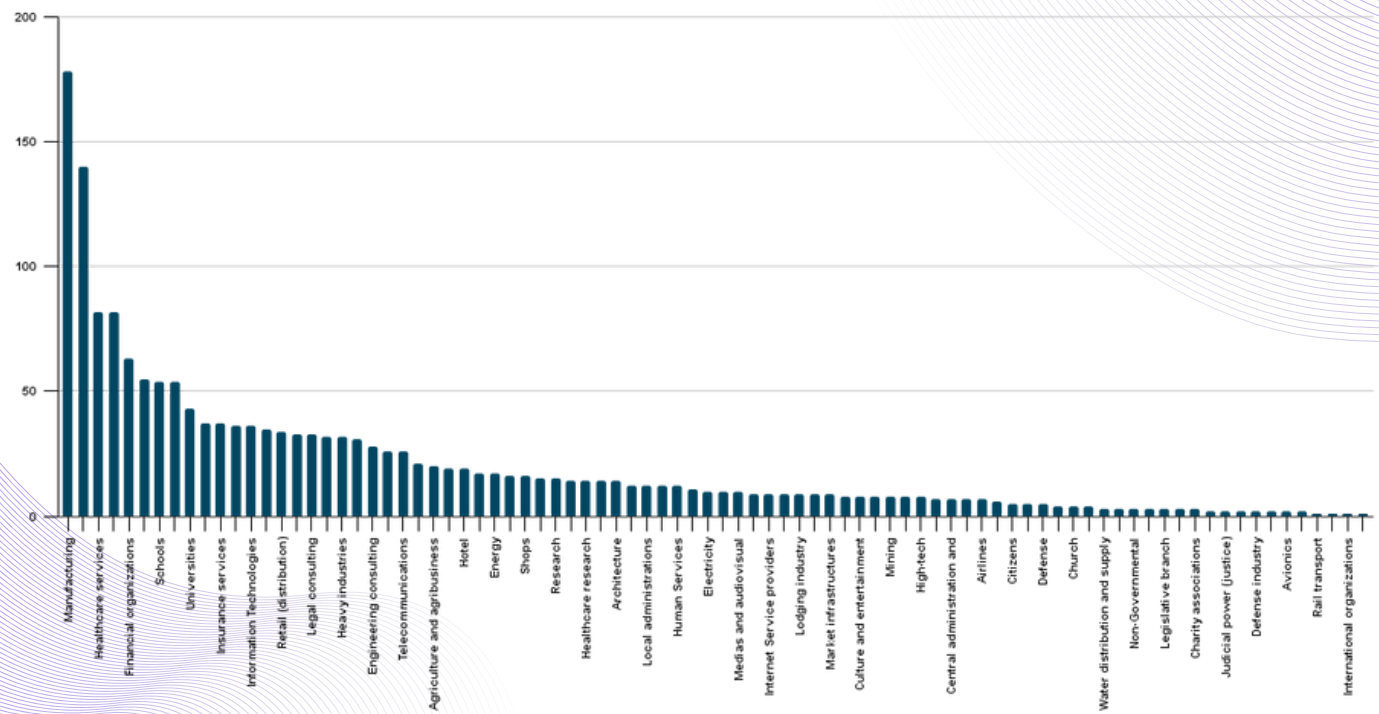
DRM
AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

DISTRIBUZIONE DEL RANSOMWARE PER SETTORI LAVORATIVI

Anche nel dato riferibile alle **categorie lavorative**, la piattaforma DRM nel quadrimestre appena trascorso, ha visto importanti novità.

Si è registrato un enrichment, risultato da una proficua collaborazione tra il nostro progetto **Ransomfeed** e **DeepDarkCTI** (guidato dall'esperto **Massimo Giaimo**), che si è preso cura di allineare tutti i dati mancanti sul settore lavorativo delle vittime coinvolte in rivendicazioni, **arricchendo di fatto il dettaglio** della nostra piattaforma.



È grazie a questo dato che, da questo quadrimestre, possiamo contare su di un set di dati di categoria **più puntuali e puri**.

Nelle **prime cinque posizioni del podio**, troviamo:

- settori produttivi industriali
- settore tecnologia
- settore sanitario
- settore costruzioni
- settore finanziario

Questi sono anche i settori che si dividono il primo grande 30% del mercato ransomware **a livello globale** (dati Q2 2023).

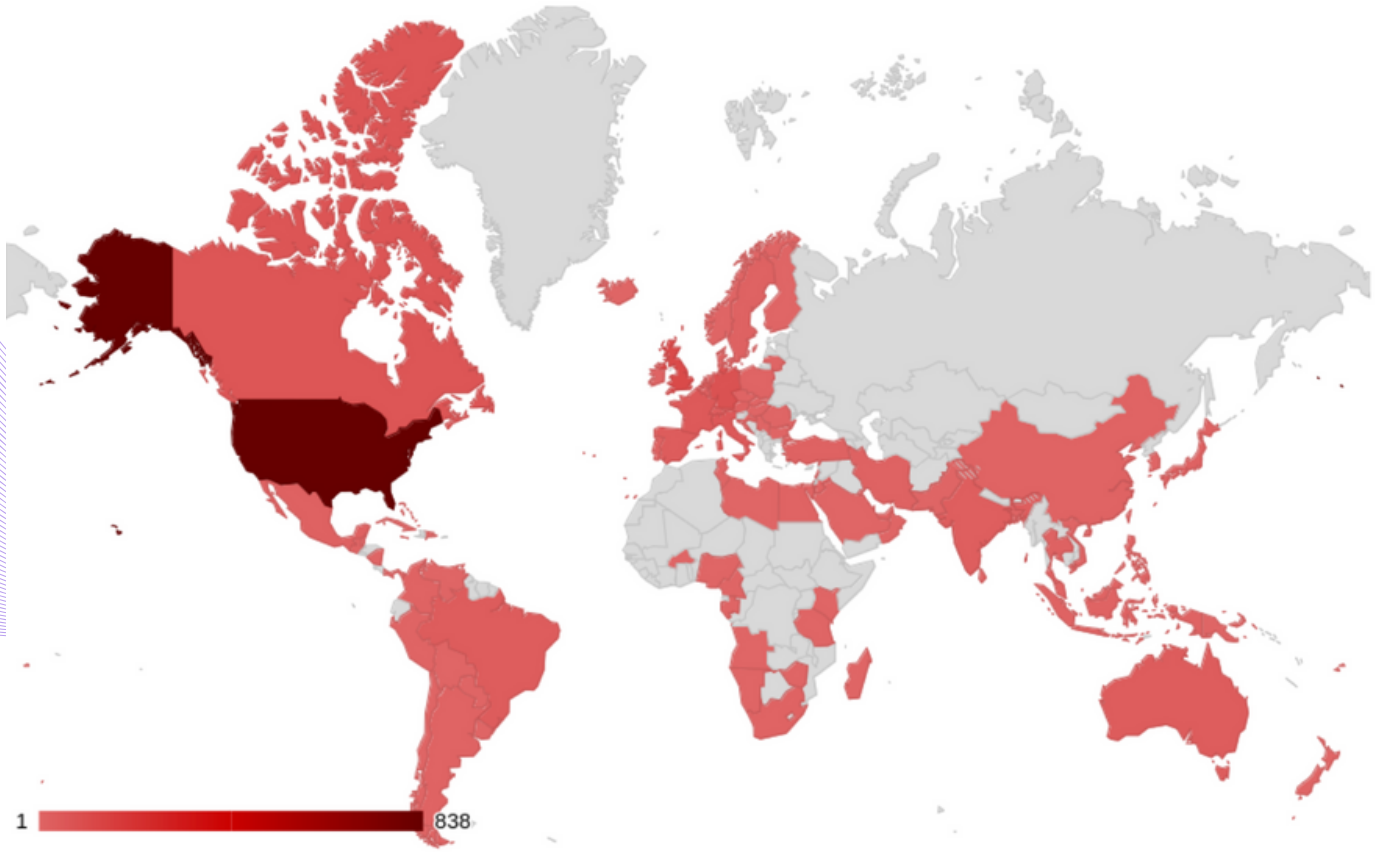
Per le categorie che impattano **sulla sicurezza nazionale**, riscontriamo che le **organizzazioni governative** in questo quadrimestre si trovano in 48esima posizione con 9 **attacchi** rivendicati. Ai quali, **se sommiamo i settori della difesa**, delle organizzazioni internazionali **governative** e il settore **giustizia**, si raggiunge il numero di **33 rivendicazioni**, che incidono per il 2% del totale.

DISTRIBUZIONE DEL RANSOMWARE NEL MONDO

Il **continuo e puntuale lavoro OSINT** che viene operato sulla piattaforma, effettuato post-scraping, permette, ad ogni quadrimestre, di avere un quadro completo sulla geografia degli attacchi informatici (partendo dalle loro rivendicazioni).

Esattamente come osservato nel Q1 2023, la fascia **nord-occidentale** del mondo si attesta 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.

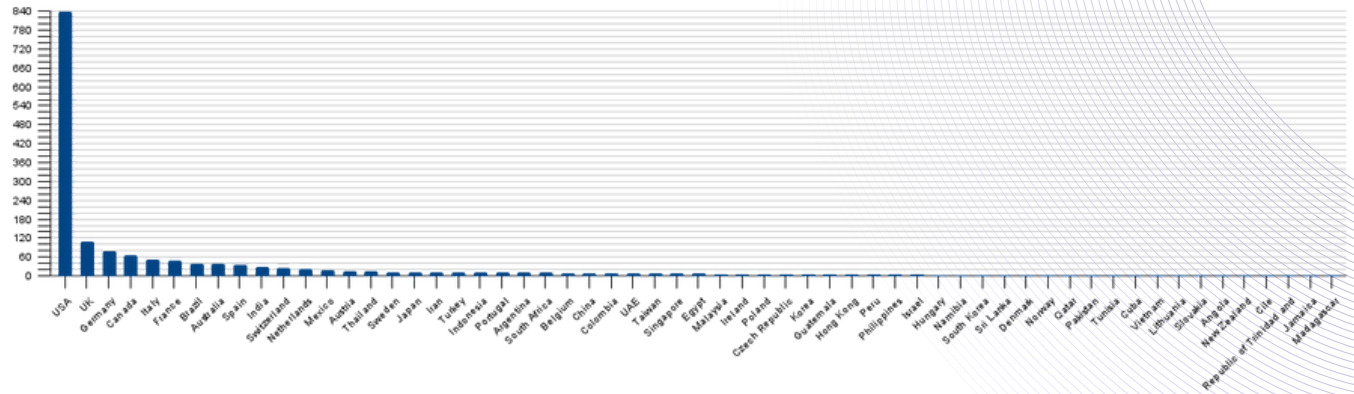


attacchi suddivisi per mese (fonte DRM)

DRM
AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

Se ci focalizziamo sulle differenze rispetto al Q1 2023, la **distribuzione geografica** è decisamente simile e in linea con il dato precedente. Si aggiunge solo il dato di Australia e Nuova Zelanda, per una nuova colorazione del continente oceanico.



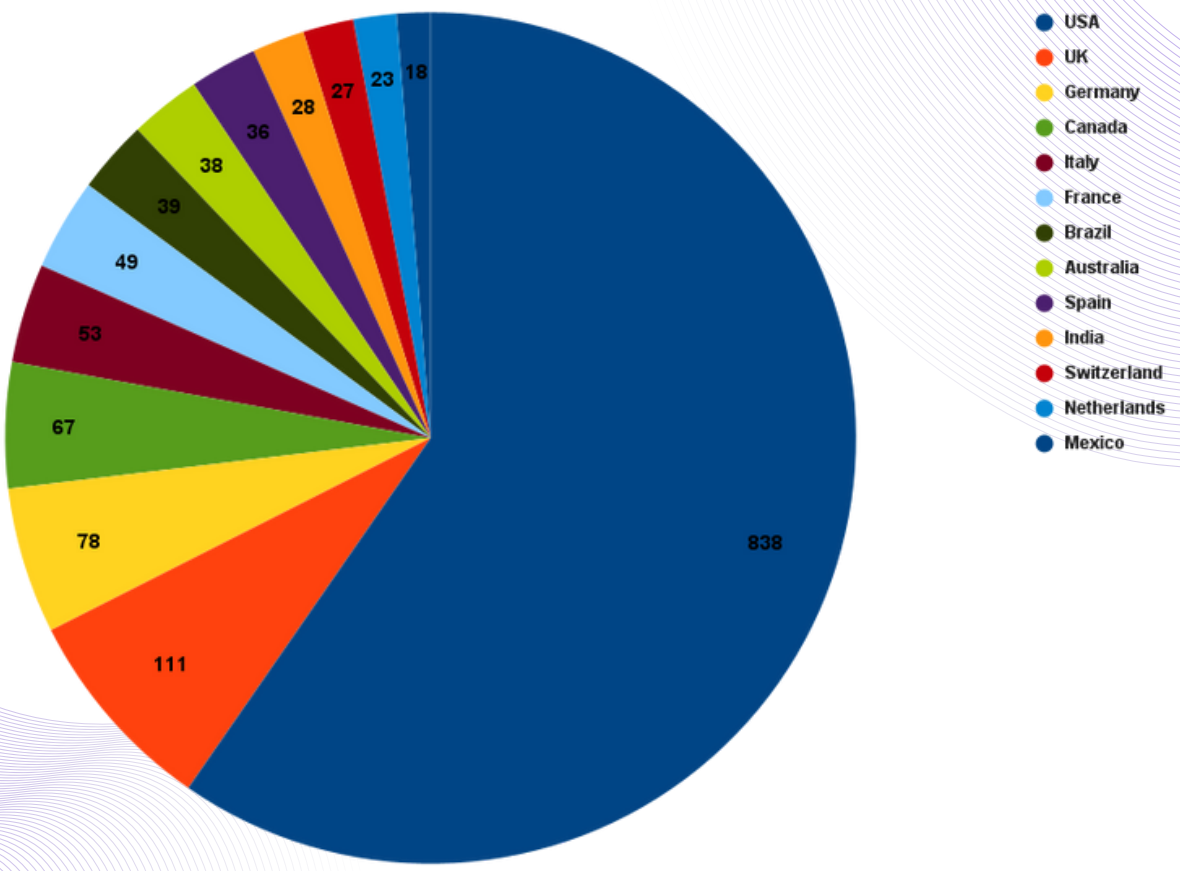
Con gli **USA** (838 attacchi) che vedono **coprire quasi il 50%** della totalità degli attacchi, le altre maggiori posizioni sono occupate nell'ordine da **UK**, **Germania** e **Canada**. L'**Italia** nel Q2 2023 si attesta in quinta posizione con 53 attacchi, salendo di una posizione - nel Q1 2023 occupava la sesta posizione.

USA	48.3%
UK	6.4%
GERMANY	4.5%
CANADA	3.9%
ITALY	3.1%

FRANCE	2.8%
BRAZIL	2.2%
AUSTRALIA	2.2%
SPAIN	2.1%
INDIA	1.6%

• TOP 13

Anche per questo segmento, aggreghiamo i dati per poterli visualizzare **escludendo i Paesi sotto l'1% di vittime ransomware** e ne rappresentiamo il grafico **per i primi 13** a livello globale, ciascuno con il numero di rivendicazioni registrate.



Il grafico **evidenzia un grande divario tra USA e resto del mondo**, divario che, facendo le dovute considerazioni rispetto alla **distribuzione industriale e di società** (possibili target) in USA, rispetto ad altri Paesi, evidenzia la capillarità dei gruppi criminali.

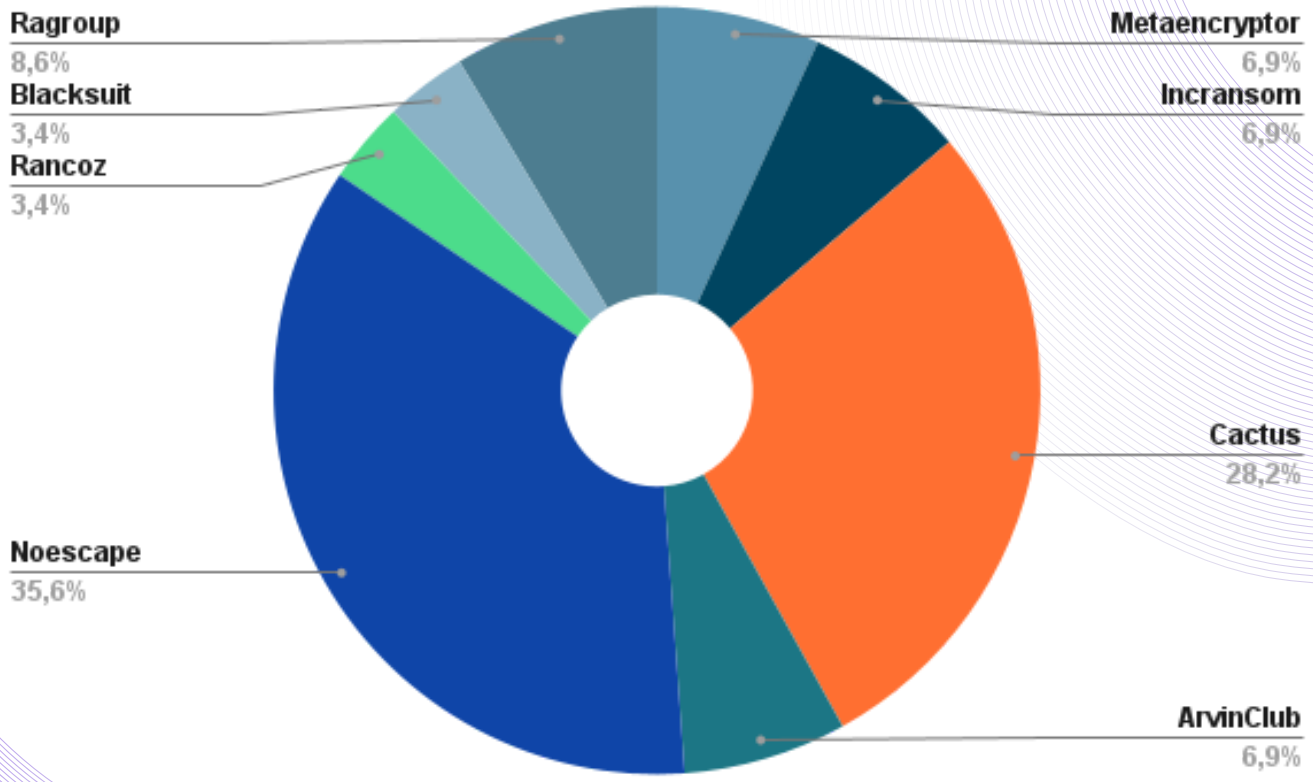
NUOVI GRUPPI CRIMINALI

Nel periodo, come spesso accade, abbiamo registrato la nascita **di nuovi gruppi** che si sono fatti spazio nella scena cyber.

DRM li ha rilevati e aggiunti al suo monitoraggio quotidiano, **totalizzando 174 nuovi attacchi** rivendicati con 8 nuovi gruppi criminali.

METAENCRYPTOR	12
INCRANSOM	12
CACTUS	49
ARVINCLUB	12
NOESCAPE	62
RANCOZ	6
BLACKSUIT	6
RAGROUP	15

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



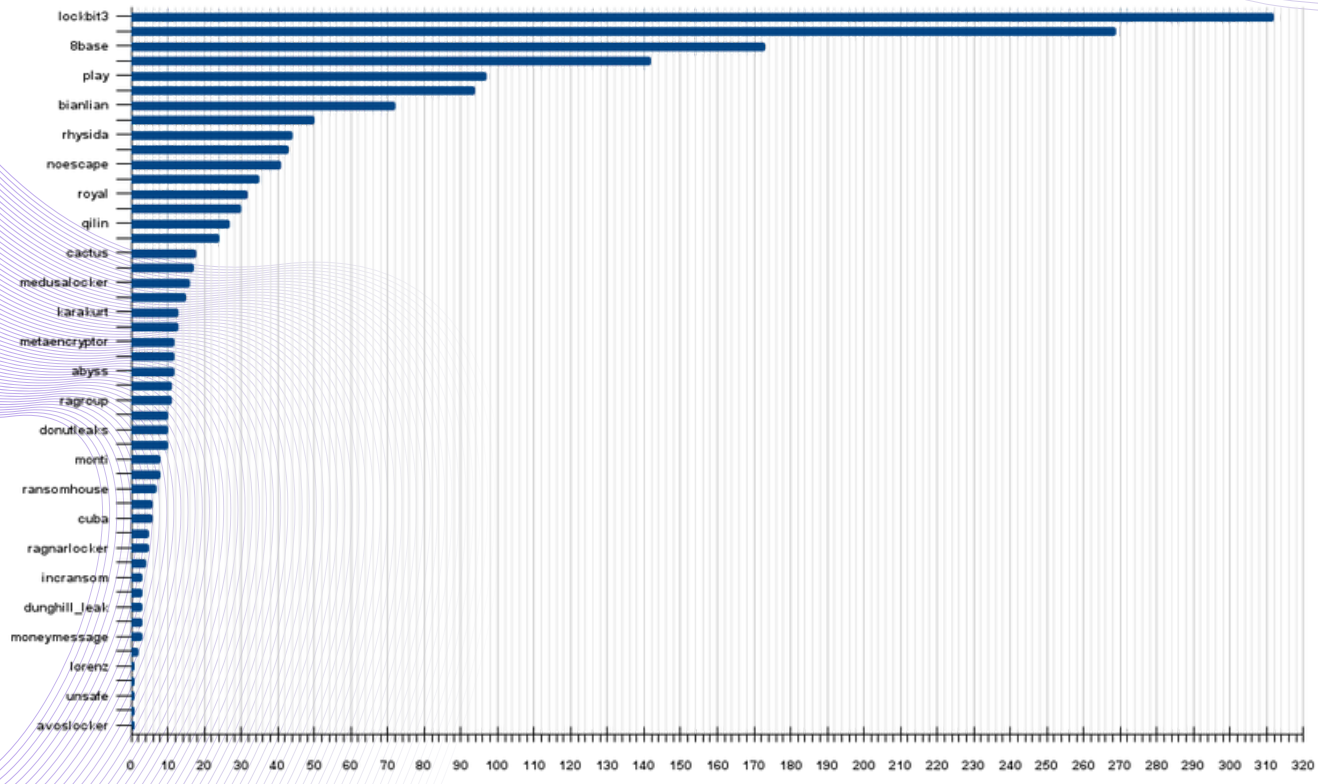
Noescape si attesta sicuramente come la nuova cyber gang più attiva nel Q2 2023, con **oltre il 35% di rivendicazioni** all'interno del suo cluster.

ATTIVITÀ GLOBALI DEI GRUPPI RANSOMWARE

Abbiamo **isolato i singoli gruppi ransomware** che hanno generato attività. Tra tutti i gruppi che costantemente vengono monitorati, la piattaforma ha rilevato **attività nel quadrimestre per 49 di questi.** Gli altri gruppi non menzionati 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 quattro gang estremamente attive, capaci da sole di **dividersi il 52%** degli attacchi.
Sono guidati da **Lockbit** che, da solo, conta il 18% degli attacchi (in calo rispetto al Q1 2023). Seguono **Clop**, **8base**, **ALPHV/BlackCa**t rispettivamente con il 15,5%, il 10% e l'8,2%.

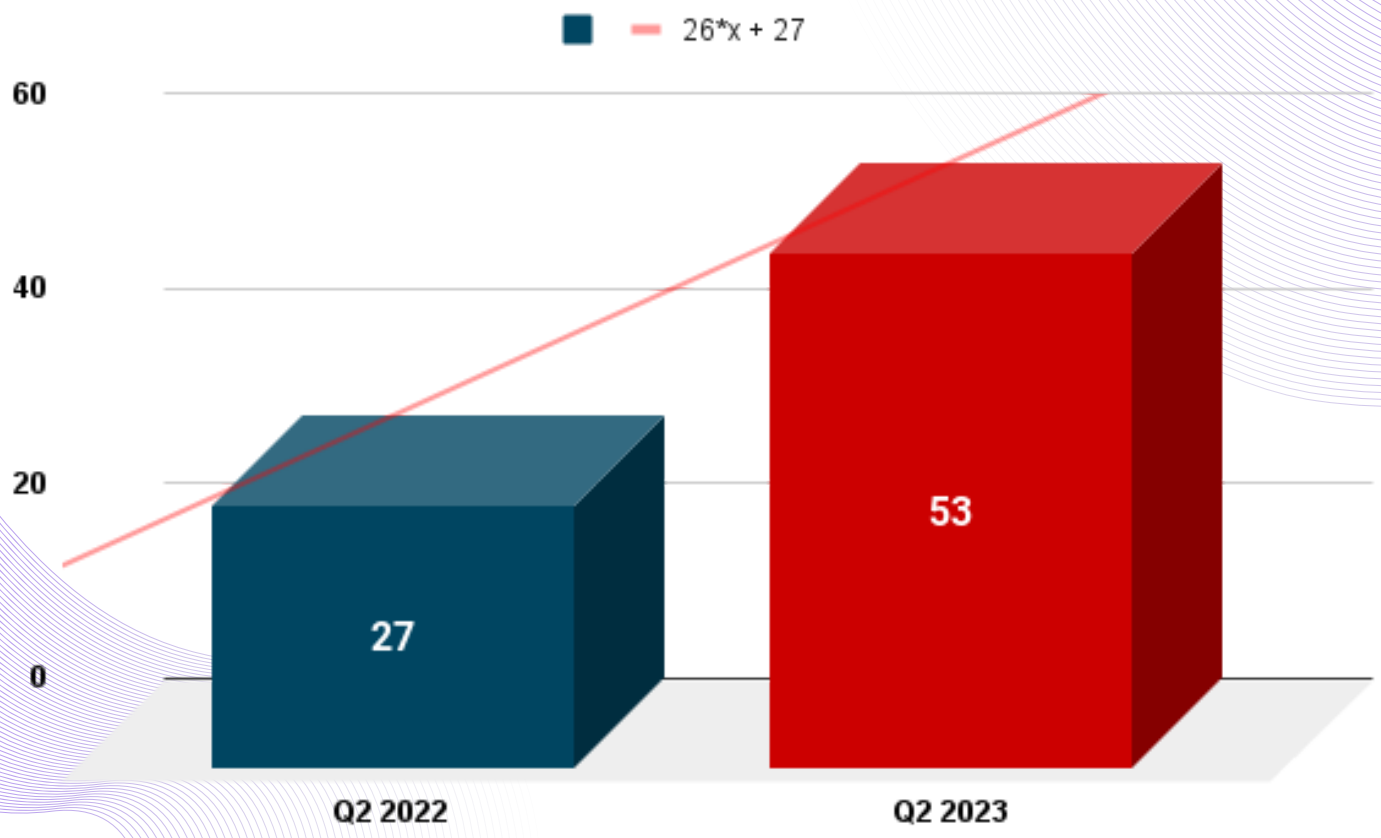
Il grafico mostra il **dettaglio di tutte le cyber gang attive**, il cui valore di riferimento è attribuito al numero di vittime rivendicate.



FOCUS ITALIA Q2 2023

In questa parte del report vengono **analizzati tutti i cluster** già visti nel dato globale, con un'attenzione particolare alla situazione dell'Italia.

Il primo dato che sicuramente emerge è il numero degli attacchi ransomware che hanno coinvolto l'Italia nel Q2 2023: sono stati 53. **Quasi uno ogni 2 giorni.**



Come per il Q1 2023, il dato **rispecchia perfettamente** il trend globale, in **costante crescita** rispetto allo stesso periodo dell'anno precedente.

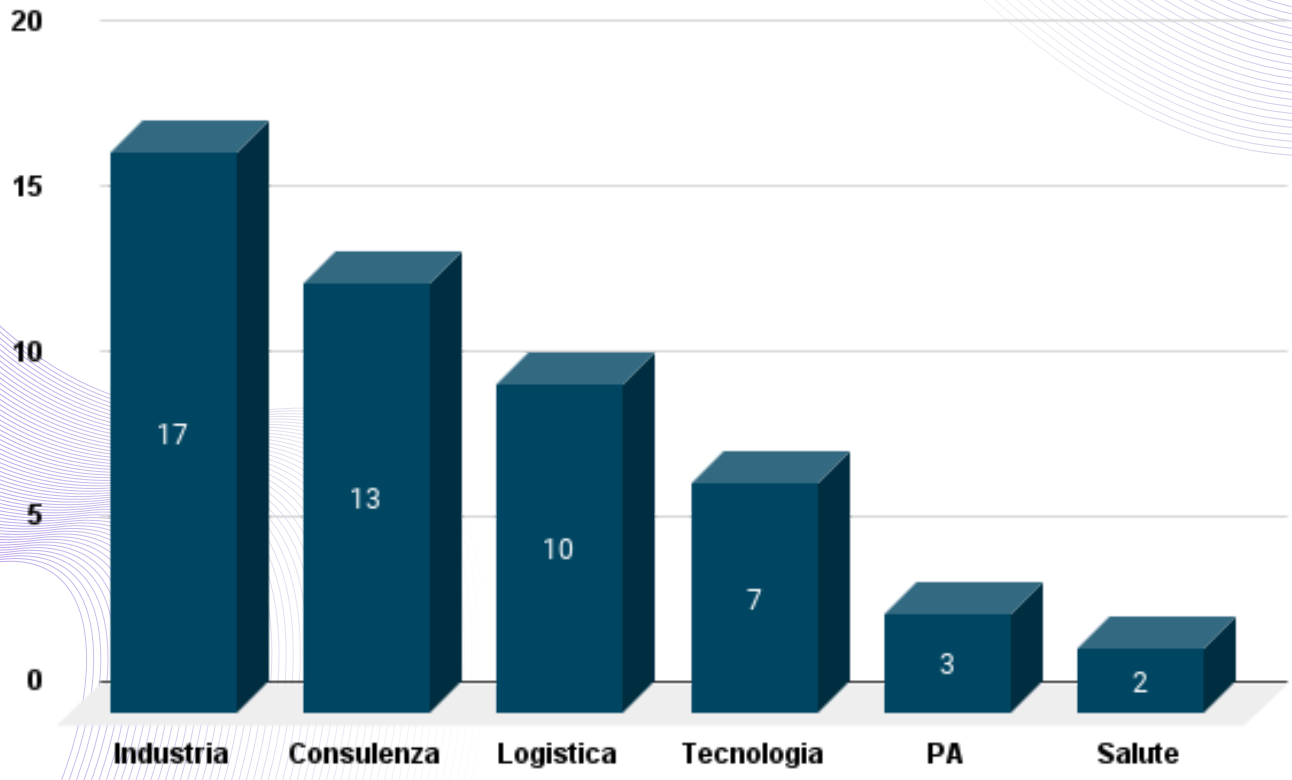
Da notare, tuttavia, che il tasso di crescita in Italia è del 96% rispetto al Q2 del 2022.

• GLI ATTACCHI PER SETTORE ECONOMICO

L'**Industria**, come nello scenario globale, si rivela il settore lavorativo più colpito anche nel focus Italia, in maniera generica (tra queste, quella **farmaceutica**, **meccanica**, **metallurgica** ed **elettronica**), con 17 **attacchi ransomware** rivendicati nel periodo.

Seguono i settori di **consulenza**, **logistica** e **tecnologia**; da rilevare che il settore della **Pubblica Amministrazione** ha impattato con sole 3 rivendicazioni.

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



In termini percentuali, possiamo leggere questi dati con l'ausilio della tabella sottostante, che ci aiuta in **fase di analisi** ad interpretarli per ogni categoria, rispetto al totale degli attacchi.

INDUSTRIA	51.5%
CONSULENZA	39.4%
LOGISTICA	30.3%
TECNOLOGIA	21.2%
PA	9.1%
SALUTE	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 periodo di riferimento.

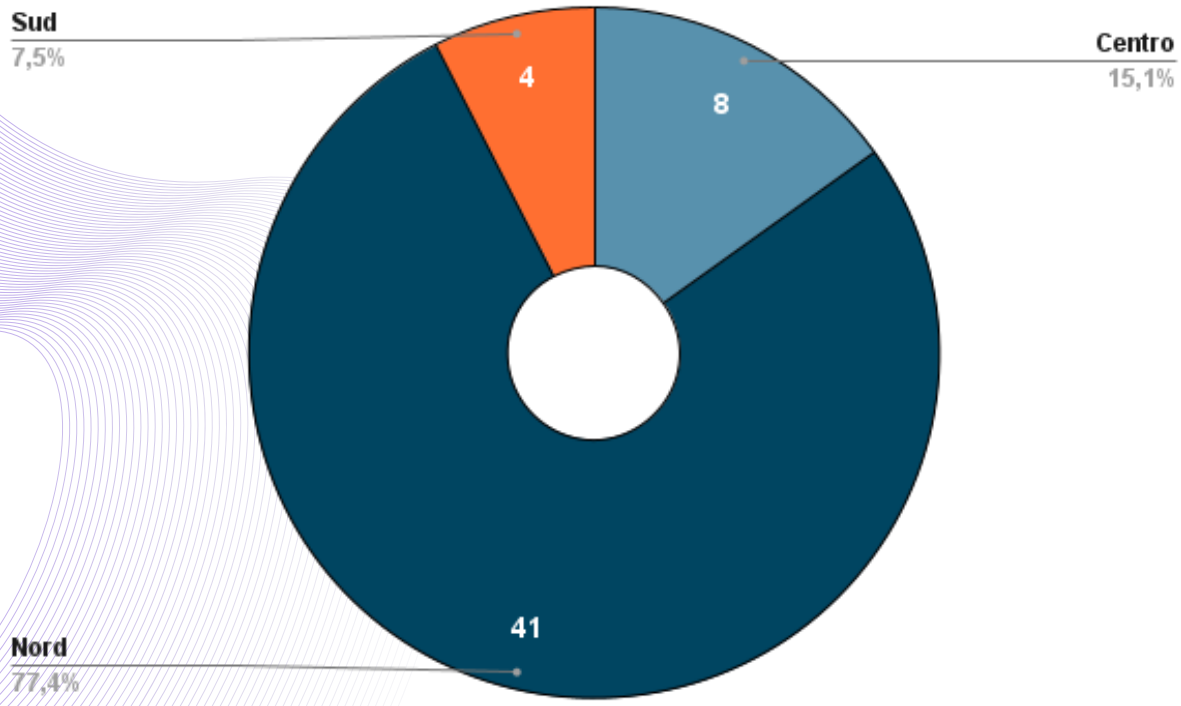
Nota: la mappa è consultabile anche online, con la funzione interattiva, cliccando sulla stessa.

Se ci si concentra su una **macrolocalizzazione** si percepisce subito l'attenzione al **nord Italia**, come dato costante nel tempo. Effettivamente anche in questo quadrimestre si parla di oltre il 77% delle rivendicazioni.

NORD	41
CENTRO	8
SUD	4

Come visto, quasi l'**80% 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.

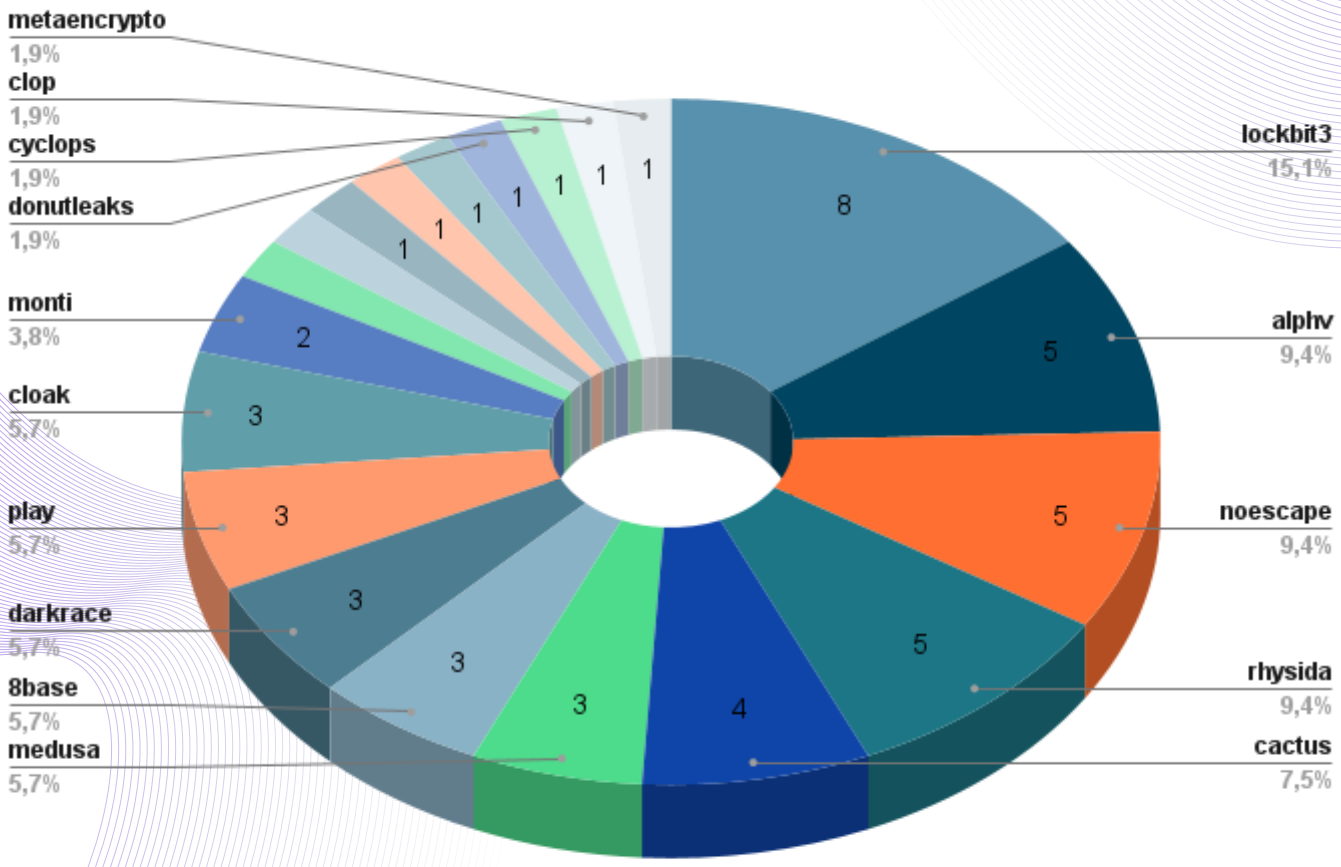


• I GRUPPI CRIMINALI PIÙ ATTIVI

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

Lockbit si attesta essere il **gruppo più attivo anche in Italia**, per il segmento considerato, con il 15% degli attacchi.

Rispetto allo scorso quadrimestre, si nota qui **una torta molto più variegata** di gruppi cyber. Non c'è infatti una netta distanza tra le attività di **Lockbit** e il resto della scena che, sembrerebbe, si sia divisa quasi in parti uguali la platea di vittime.



Si possono notare gli attacchi **verso i target italiani**, con le percentuali di ogni gruppo e, all'interno, con il numero di vittime rivendicate.

CONCLUSIONE

Il secondo quadrimestre del 2023 ha rappresentato un periodo di **crescente preoccupazione** nel panorama delle minacce ransomware, con numerose organizzazioni ed enti in tutto il mondo che hanno subito attacchi devastanti.

La **piattaforma DRM** ha svolto un ruolo cruciale nel monitoraggio e nella raccolta di dati pertinenti, evidenziando l'attività di **165 gruppi criminali** e l'identificazione di **1736 rivendicazioni** ransomware, di cui **53 solo in Italia**.

La localizzazione geografica e il settore lavorativo delle vittime hanno fornito informazioni preziose per la comprensione dei trend e delle minacce emergenti. In particolare, gli attacchi ransomware in Italia richiedono un'attenzione continua e strategie di **mitigazione avanzate per garantire la sicurezza** delle organizzazioni nazionali.

Questo report offre una panoramica dettagliata di questi eventi, con l'obiettivo di supportare gli sforzi nel rafforzamento della sicurezza informatica e nella prevenzione di futuri attacchi ransomware.

DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

DASHBOARD RANSOMWARE MONITOR

Dashboard Ransomware Monitor (DRM) è un servizio di monitoraggio dei gruppi ransomware; utilizzando l'attività di scraping, ovvero l'estrazione di dati da più siti web per mezzo di programmi software e la successiva strutturazione degli stessi, la DRM memorizza le rivendicazioni in un feed RSS permanente, disponibile per la libera consultazione.

Il servizio di monitoraggio è fruibile da tutti, **gratuito**, e raccoglie e analizza costantemente i dati relativi agli attacchi ransomware a livello internazionale.

La piattaforma è in grado di rilevare in modo tempestivo gli attacchi e analizzarne i pattern, mettendo i dati a disposizione di chiunque desideri comprendere l'entità e l'evoluzione degli attacchi informatici.

Per saperne di più: **ransomfeed.it**

DRM

AN ITALIAN PROJECT

DASHBOARD RANSOMWARE MONITOR

RANSOMFEED | RANSOMFEED.IT