Swascan
TINEXTA GROUP

Q4 e Round-up Ransomware 2022

SOMMARIO

EXECUTIVE SUMMARY

753 obiettivi attaccati con dati pubblicati (che non hanno pagato il riscatto) in **77 paesi** nel quarto trimestre di quest'anno. 41 i gruppi ransomware che utilizzano il data leak in attività censiti tra ottobre e dicembre, con **una crescita del 13%** rispetto ai 36 del trimestre precedente.
In questo contesto, Il **SOC & Threat Intelligence Team di Swascan** ha intrapreso un'analisi del profilo delle vittime finite nel mirino delle gang di Criminal Hackers nel **Q4 2022.**

In questa analisi quando vengono menzionate le numeriche inerenti alle vittime, sono state prese in considerazione unicamente quelle entità che non solo hanno subito un attacco ransomware, ma si sono viste anche vittime di Data Leak tramite double extortion.

In particolare, sono stati raccolti, attraverso specifiche ricerche **OSINT & CLOSINT,** i dati che riguardano le vittime delle **15 gang Ransomware più attive** nel quarto trimestre del 2022:

LockBit	Alphav/ BlackCat	Royal	BlackBasta	BianLian
Karakurt	PLAY	Hive	Vice Society	Snatch
LV	SiegedSec	Cuba	RagnarLocker	BlackByte

Metodologia in breve

L'approccio metodologico utilizzato è stato il seguente:

1. identificazione dei siti Darkweb delle relative gang Ransomware;
2. individuazione delle aziende vittime che sono state pubblicate sui portali Darkweb;
3. clusterizzazione delle informazioni relativamente alle vittime in termini di:

- **Area geografica**
- **Settore merceologico**
- **Fatturato e dipendenti**

Q4 In breve

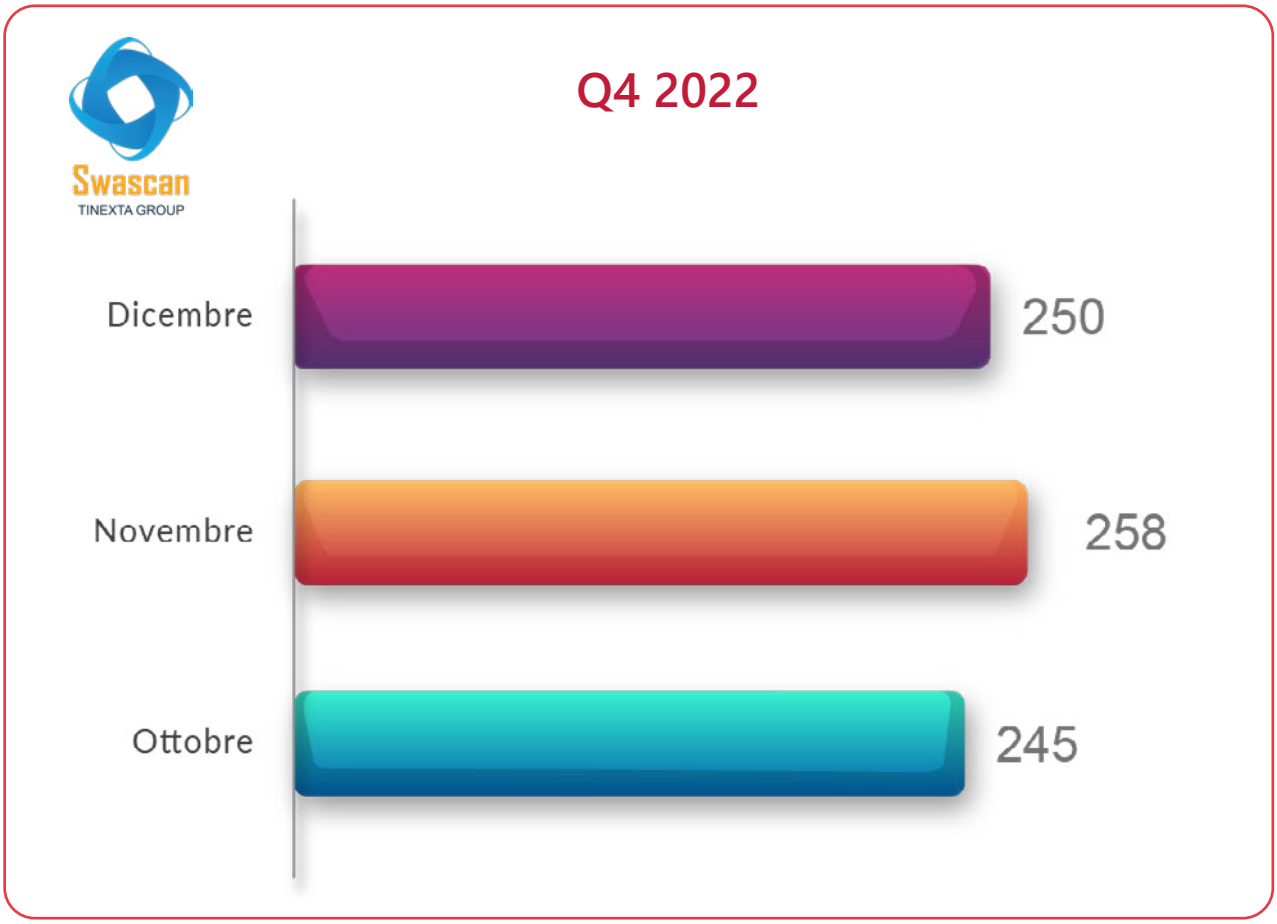
Focalizzandoci sul Q4 2022, si riscontrano:

1. **+122% di vittime** che hanno visto i propri dati pubblicati dall'inizio dell'anno, passando da 112 vittime nel mese di gennaio a 249 nel mese di dicembre.

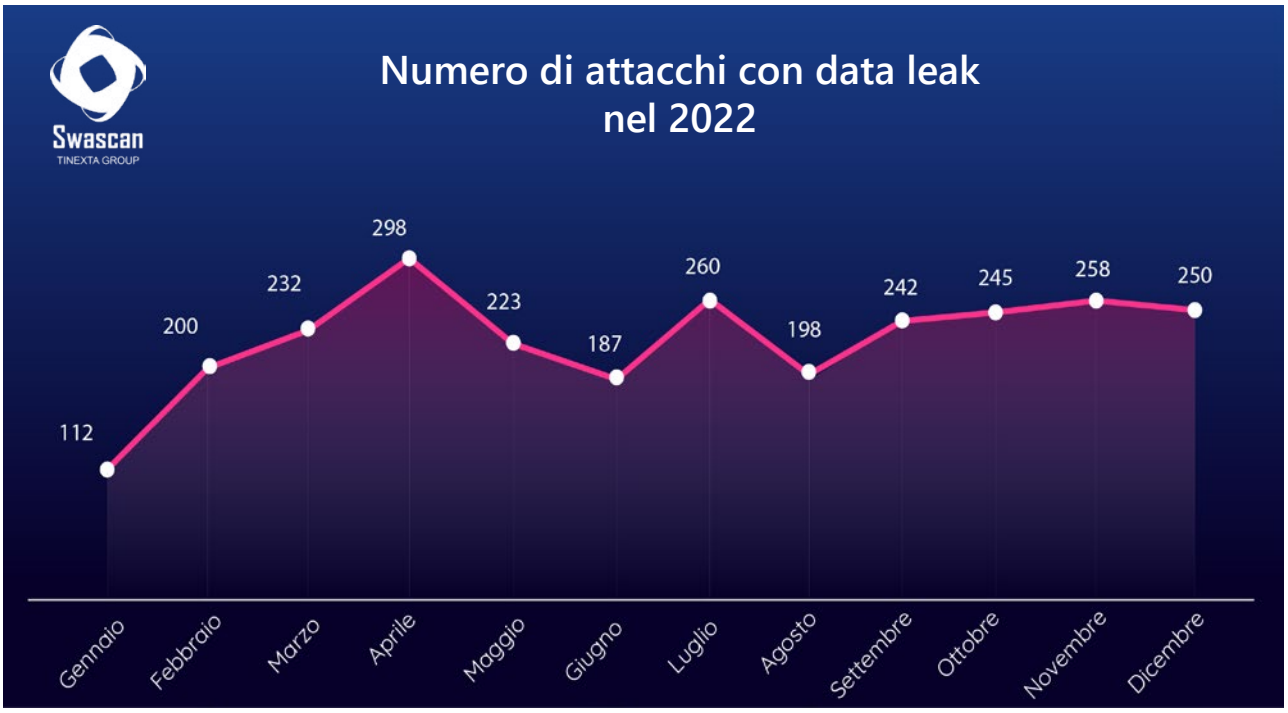
2. **Diminuzione di vittime** delle aziende con dati pubblicati **in Italia** ispetto al Q3 2022 dove il totale delle aziende colpite con annesso data leak era di 29, mentre nell'ultimo trimestre scendono a 14.

3. **Numero costante** di vittime negli **Stati Uniti**, che mantiene il primato per numero di attacchi.

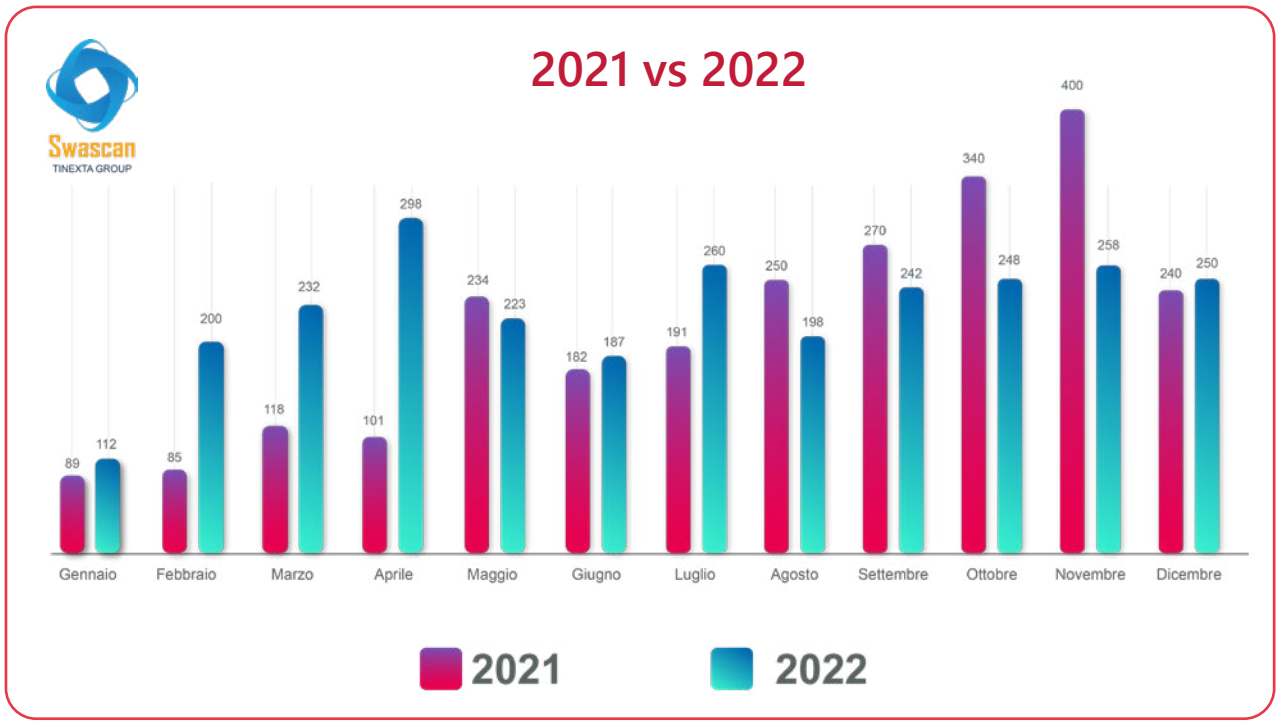
Dopo un calo di attacchi nel mese di agosto e una risalita nel mese di settembre, l'ultimo trimestre del 2022 vede un numero costante di attacchi: in cima al medagliere sempre gli Stati Uniti che raggiungono un totale di 275 vittime e la gang LockBit che conta un totale di 149 attacchi rivendicati.



Aprile è stato il mese con **più attacchi** correlati da successivo data leak **nel 2022 (298),** mentre a gennaio il totale era di 112, con una crescita del +166%. Altri due picchi a **luglio (260)** e **novembre (258).**



Tuttavia, rispetto al 2021, anno in cui **l'attività delle gang ransomware** è **cresciuta** in modo esponenziale nell'ultimo trimestre, comparando il Q4 2021 e il Q4 2022 riscontriamo **un calo di attacchi** con dati pubblicati **del -23.7%.**



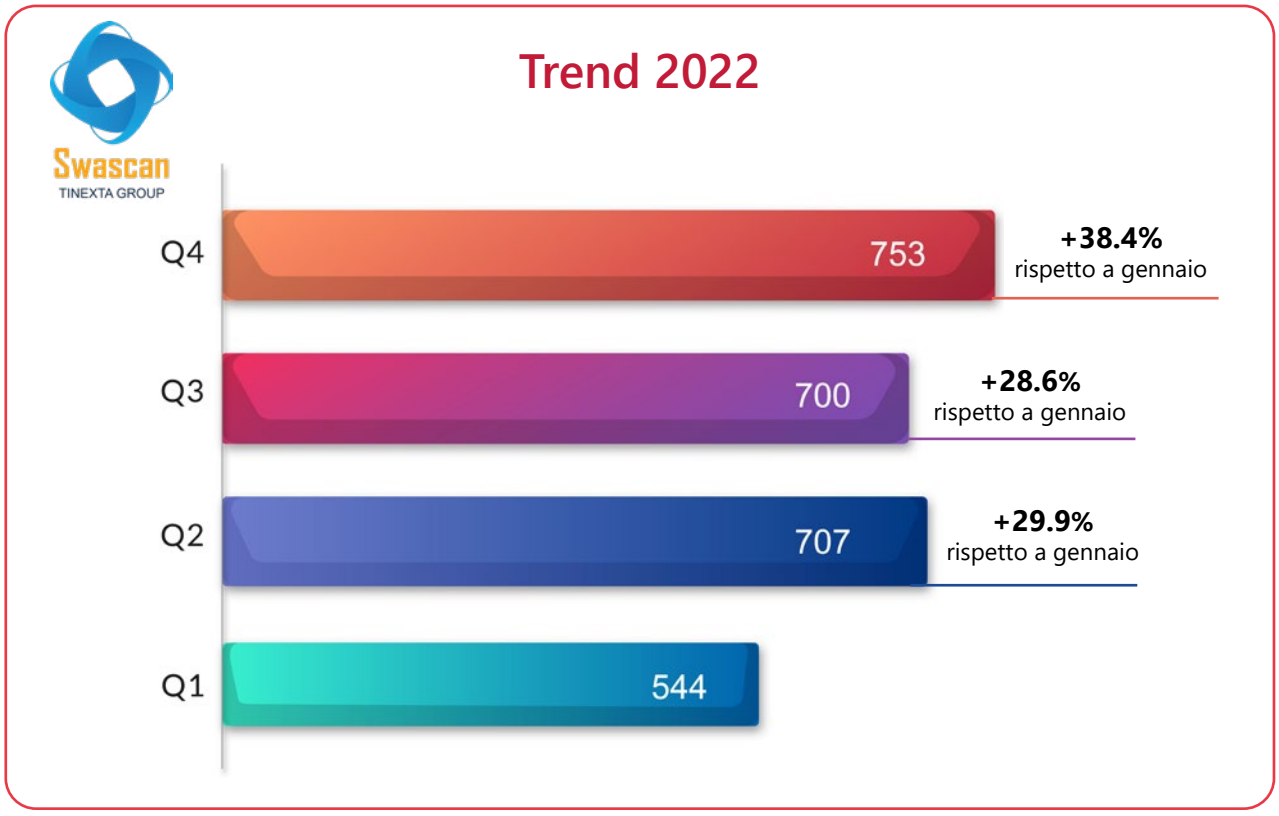
Riportiamo di seguito una tabella riassuntiva confrontando il Q3 vs Q4 2022:

	Q3 2022	Q4 2022	Q4/Q3 (in %)
Vittime di Data Leaks	700	753	+7.5%
Gruppi di ransomware totali	36	41	+13%
Vittime di LockBit con data leak	234	149	-36%
Paese più colpito	United States	United States	
Totale Paesi colpiti	76	77	+1%
I 5 paesi più colpiti	United States, France, Spain, United Kingdom, Germany	United States, United Kingdom, Canada,Germany, Brazil	
Settori più colpiti	Services	Services	
PMI colpite	82%	84%	+2%

www.swascan.com
info@swascan.com

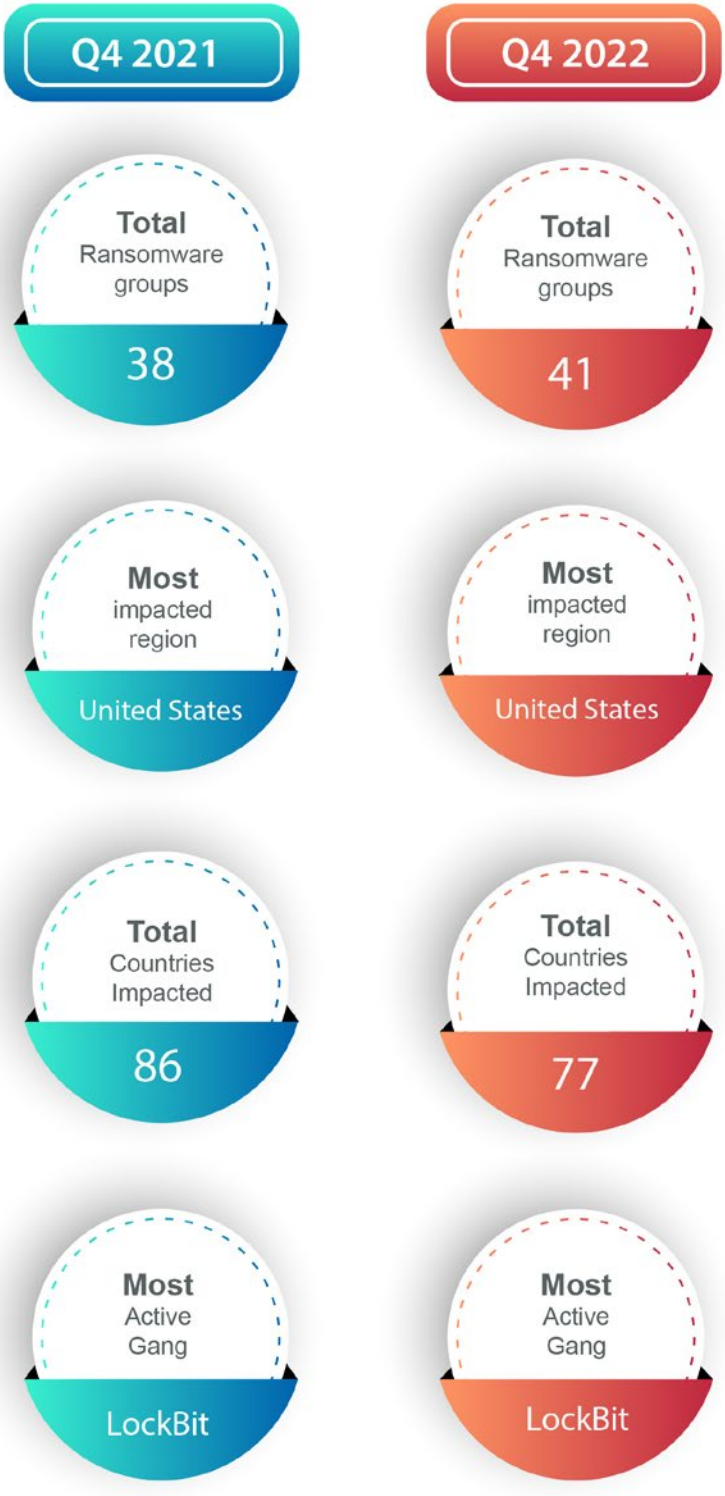
IL CONTESTO

A livello globale, è possibile osservare come nel **quarto trimestre del 2022 il numero di vittime** pubblicate raggiunga i **753 casi**, con un **incremento del 7.5%** rispetto al Q3 dove si contavano 700 attacchi, ma un **decremento del 23% rispetto al Q4 2021** dove il numero di aziende colpite raggiungeva un totale di 986.
Cresce invece il **numero delle gang attive**, per un totale di **41** nell'ultimo trimestre (**+17%** rispetto ad inizio anno):



Swascan
TINEXTA GROUP

2021 vs 2022



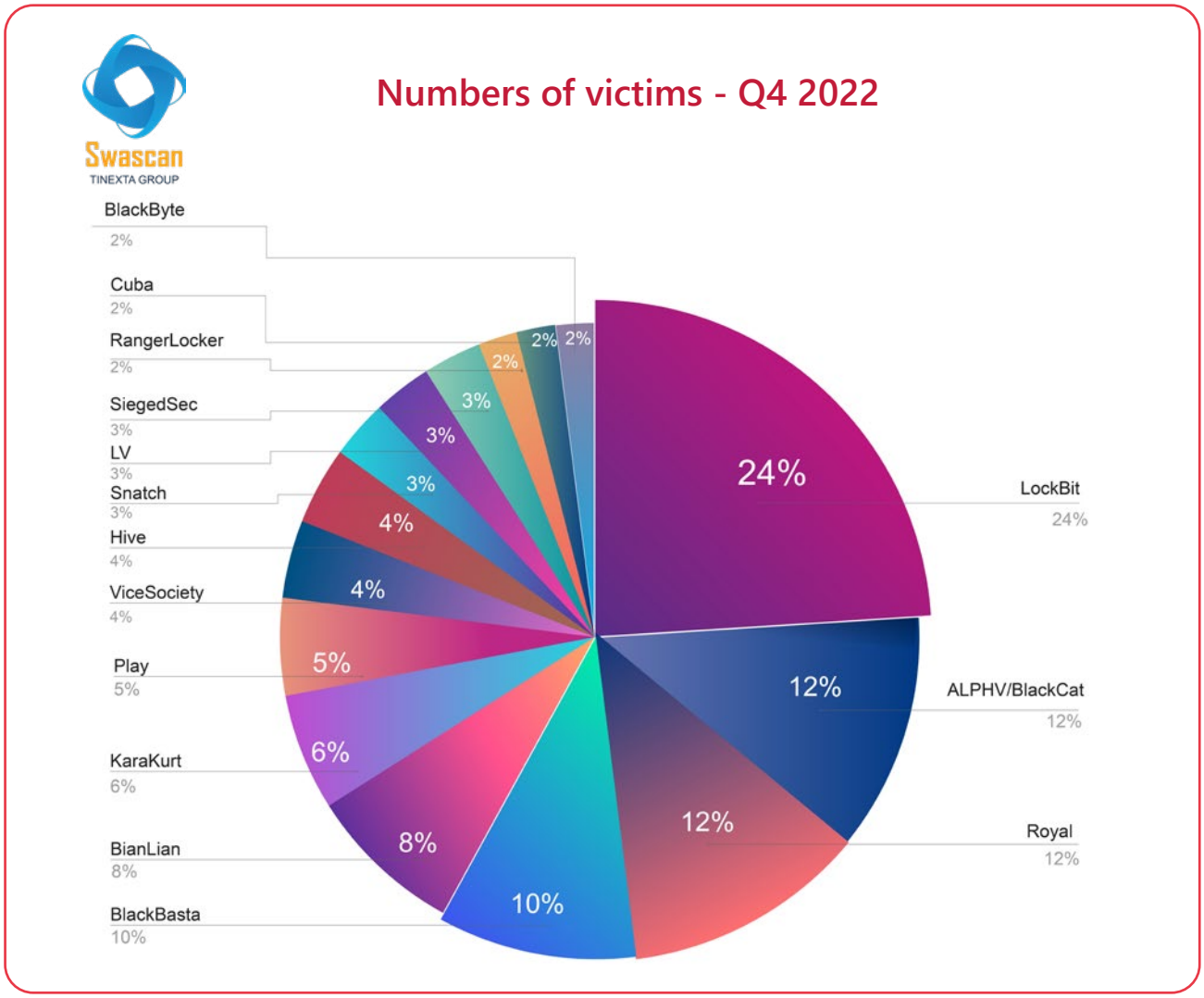
www.swascan.com
info@swascan.com

LE GANG RANSOMWARE PIÙ PROLIFICHE

Nel quarto trimestre **La gang LockBit** continua a spiccare per numero di attacchi con data leak **(149),** nonostante un notevole **decremento (-39%)** rispetto al trimestre precedente dove si contavano 234 vittime: malgrado ciò, LockBit continua ad essere primo nella classifica di gang più attive, l'attività risulta , raggiungendo un totale di **817 vittime nel 2022.**

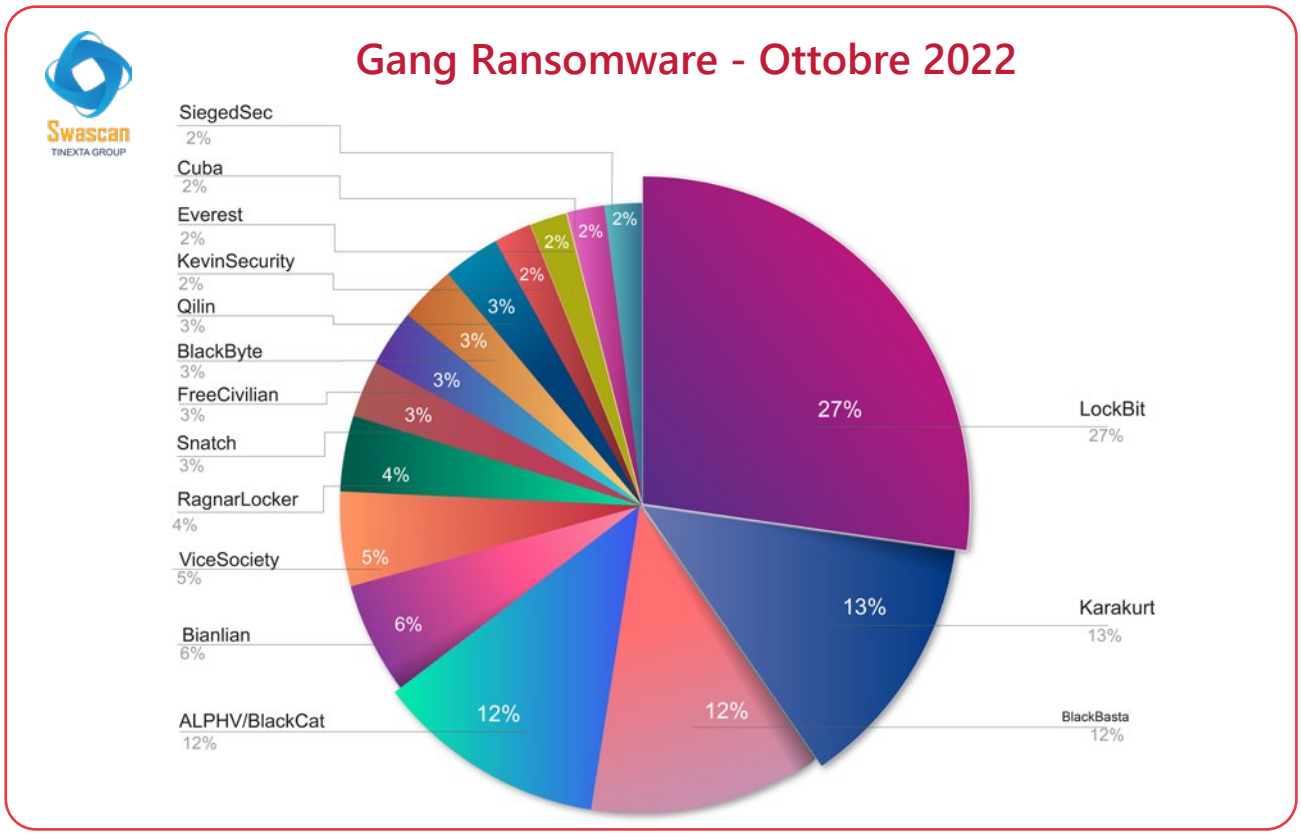
Scorrendo la classifica, al secondo posto con oltre **77 attacchi** messi a segno spicca la **gang ALPHAV/BlackCat mentre** seguita da **Royal** con **76 vittime** mentre nel Q3 la seconda posizione era di Blackbasta.

Di seguito la classifica delle gang ransomware più attive:

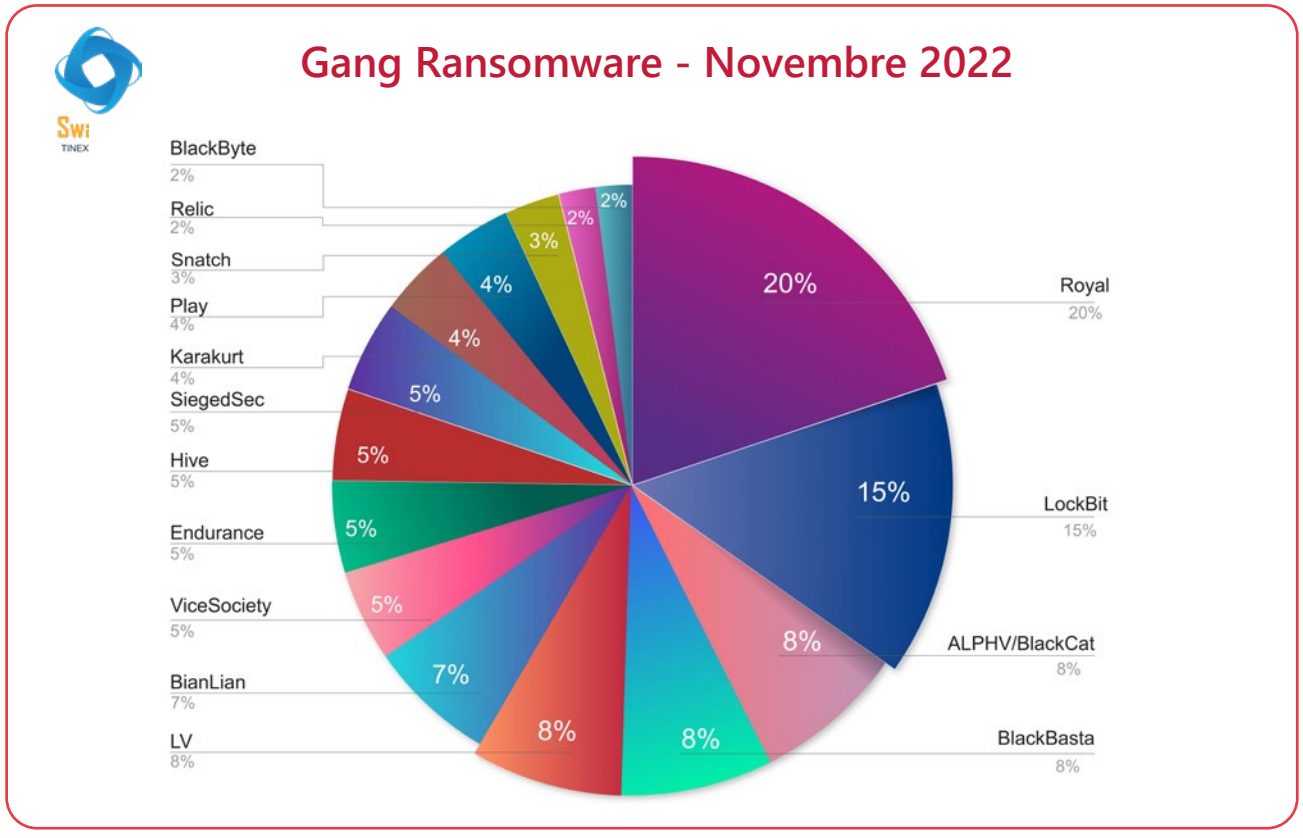


Di seguito riportiamo l'analisi relativa ad ogni singolo mese del Q4 2022.

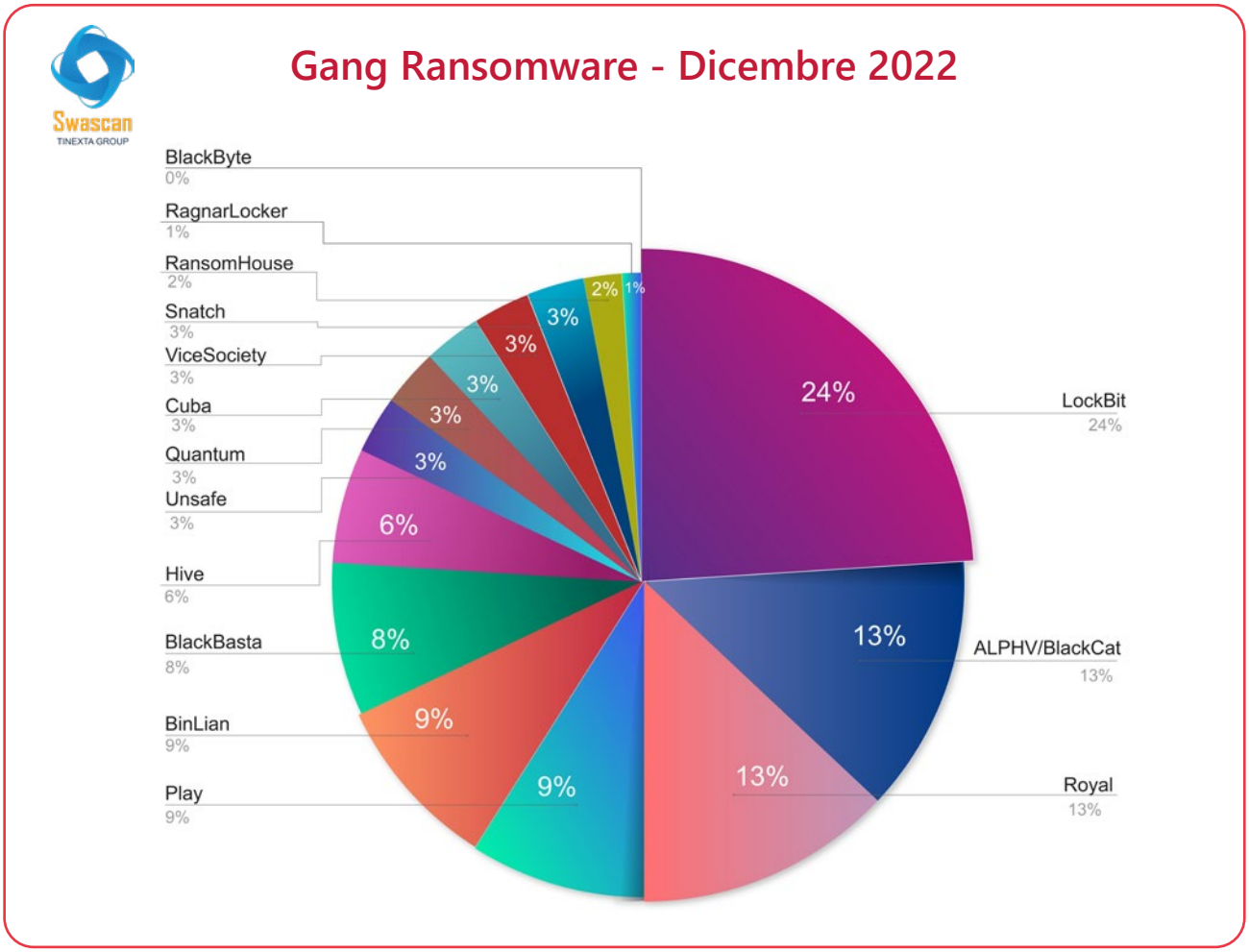
Per il solo mese di **ottobre 2022,** queste le gang ransomware più attive:



Nel mese di **novembre 2022**, con un totale di **46 vittime**, la gang Royal sorpassa LockBit che passa per la prima volta nel corso del 2022 al secondo posto:



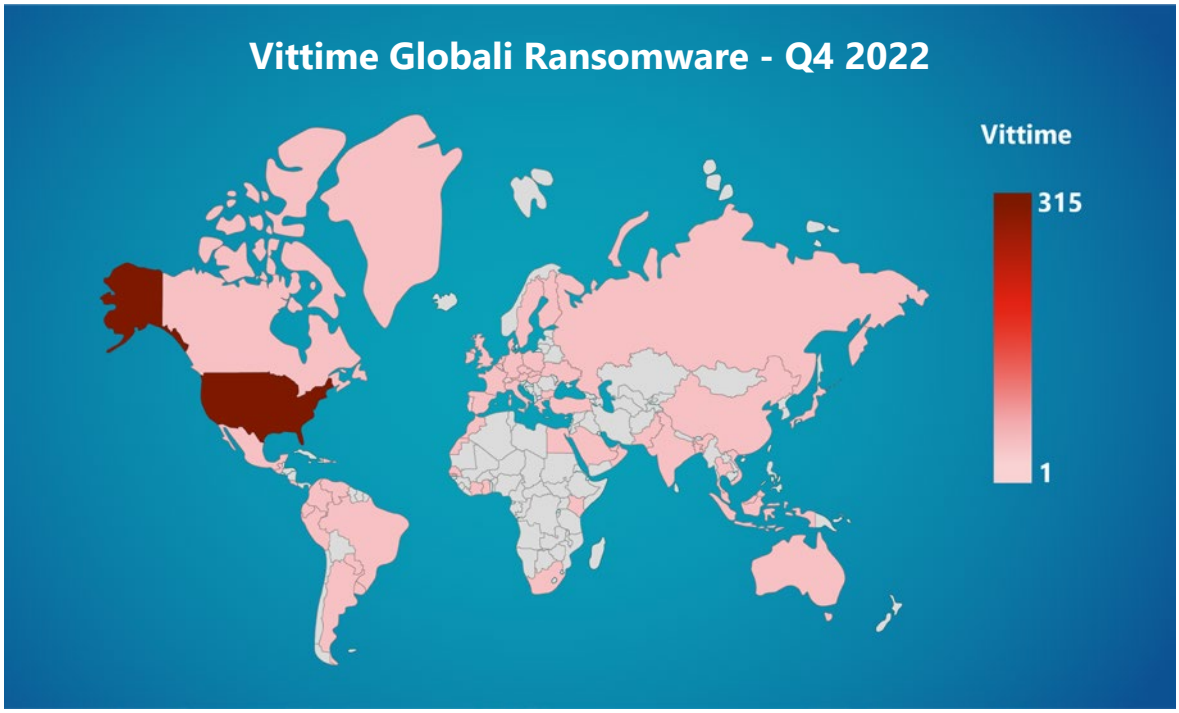
Per il mese di **dicembre 2022,** queste le gang ransomware più attive, con la comparsa della nuova gang **"Unsafeleak"** che si posizione all'ottavo posto nella classifica mensile:



DISTRIBUZIONE GEOGRAFICA DELLE VITTIME

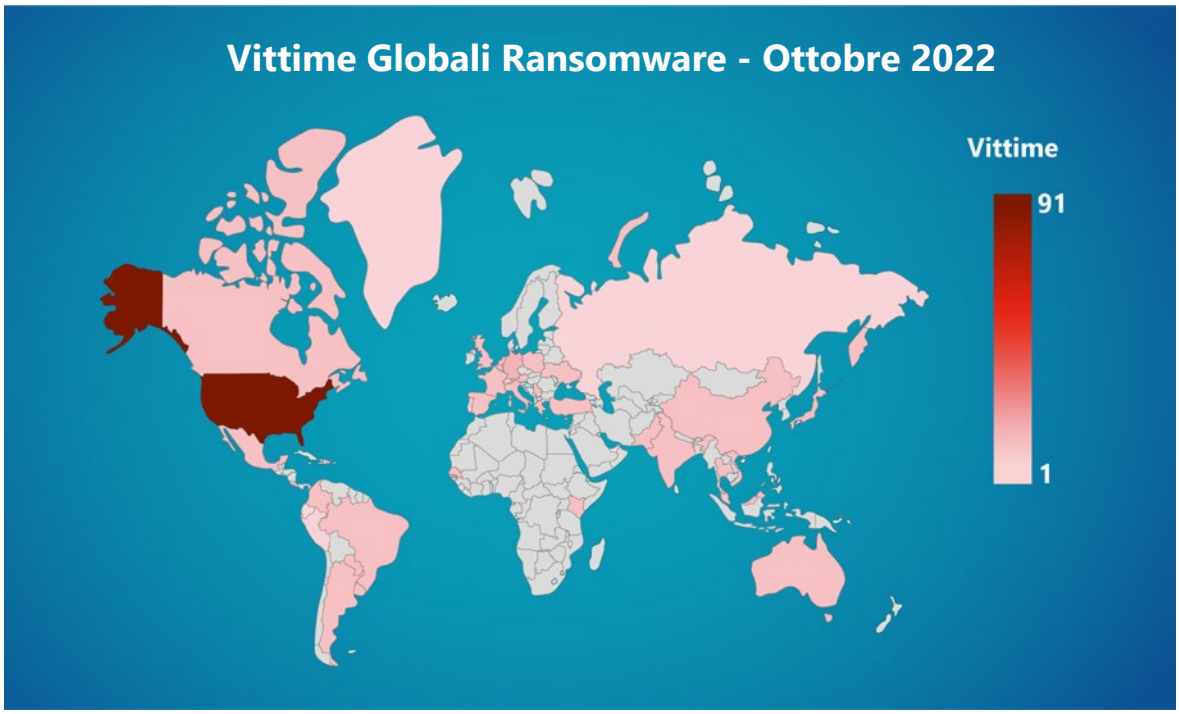
Gli **Stati Uniti** si confermano al **primo posto** con un totale di **275 attacchi** nel corso dell'ultimo trimestre del 2022, mentre **l'Italia scende al 10°** posto (rispetto al sesto del mese precedente). Tra i paesi europei passa al primo posto la **Germania** con un totale di **29 aziende che non hanno accetatto di pagare il riscatto**

Nelle mappe di seguito, la distribuzione geografica degli attacchi ransomware nel quarto trimestre 2022.



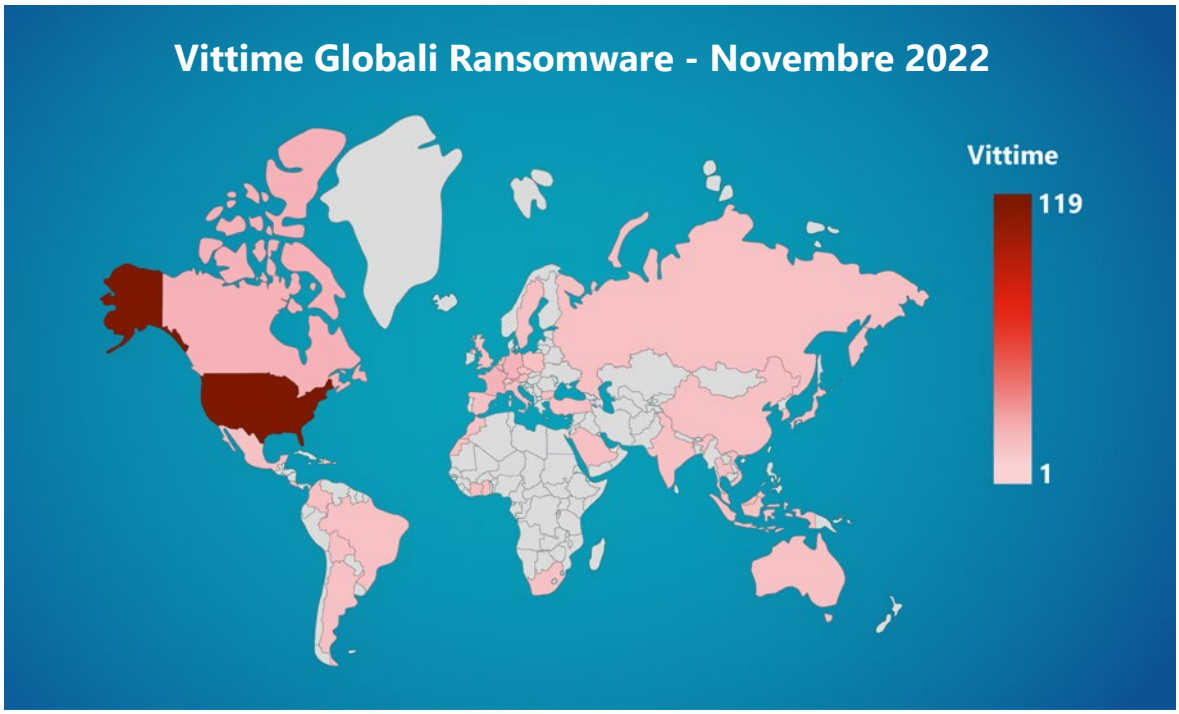
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Q4 2022
United States	62%
United Kingdom	8%
Canada	8%
Germany	6%
Brazil	4%
Australia	4%
France	4%
India	3%

Nel mese di **ottobre** si contano un totale di **91 vittime** negli **Stati Uniti**. Nello stesso mese, in **Italia** il numero di **aziende colpite è 7.**



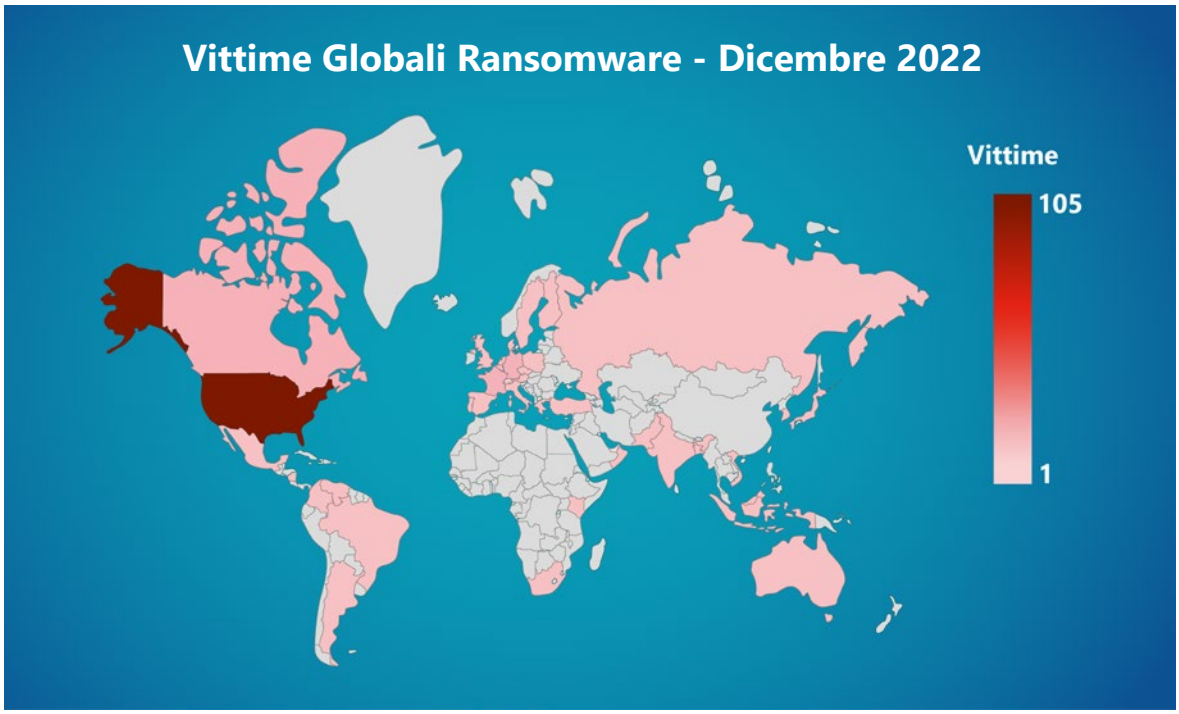
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – ottobre 2022
United States	58%
United Kingdom	10%
Germany	7%
Australia	6%
Brazil	5%
France	4%
Italy	4%
Mexico	4%

Stesso di scorso per il mese di novembre, in cui gli **Stati Uniti** contano un totale di **119 vittime**. Scendono invece le aziende che non hanno accettato di pagare il riscatto in **Italia,** per un totale di **2** nel mese preso in analisi.



PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – novembre 2022
United States	64%
Canada	11%
United Kingdom	6%
Germany	5%
India	4%
Brazil	3%
France	3%
Indonesia	3%

Anche a **dicembre 2022** il più alto numero di vittime è riscontrato negli **Stati Uniti (105)**. Nello stesso mese, in **Italia** se ne contano **5**.



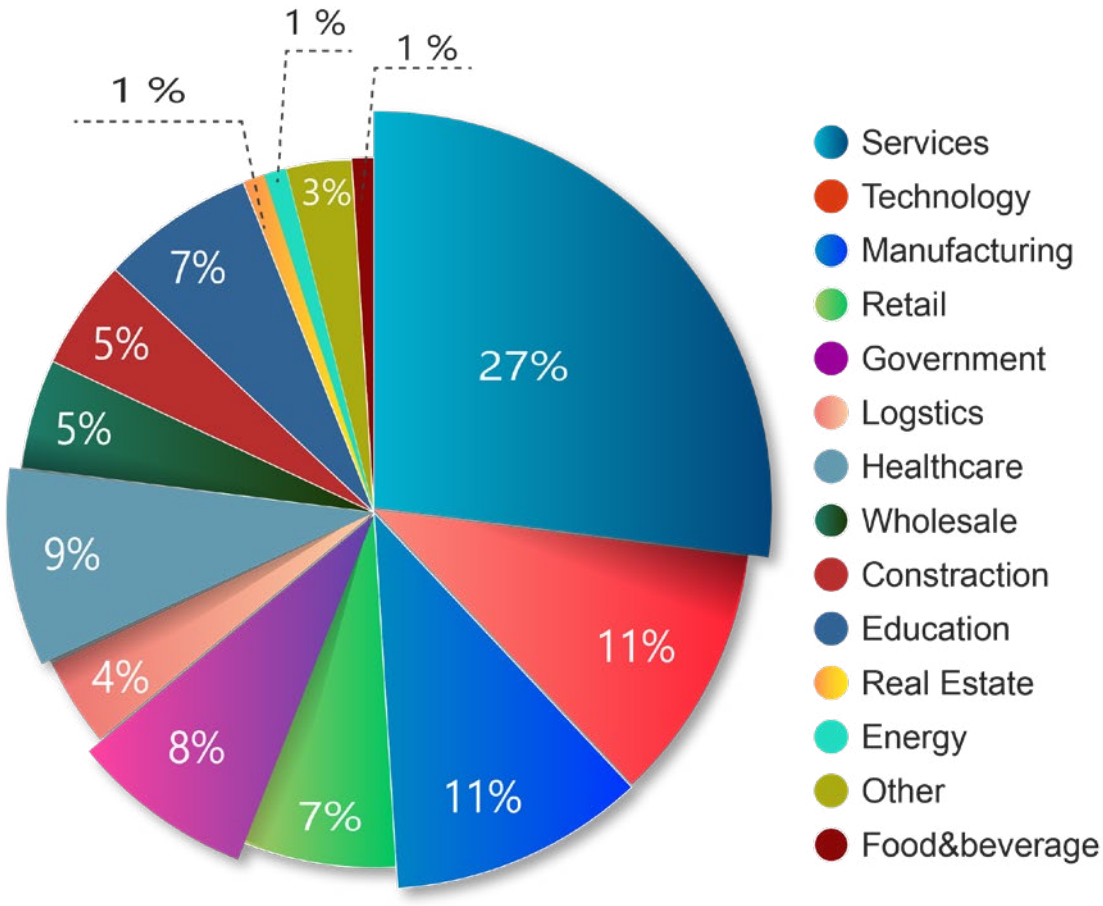
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – dicembre 2022
United States	62%
Canada	8%
United Kingdom	8%
Germany	5%
Brazil	5%
Australia	4%
France	4%
New Zeland	4%

I SETTORI PRESI DI MIRA

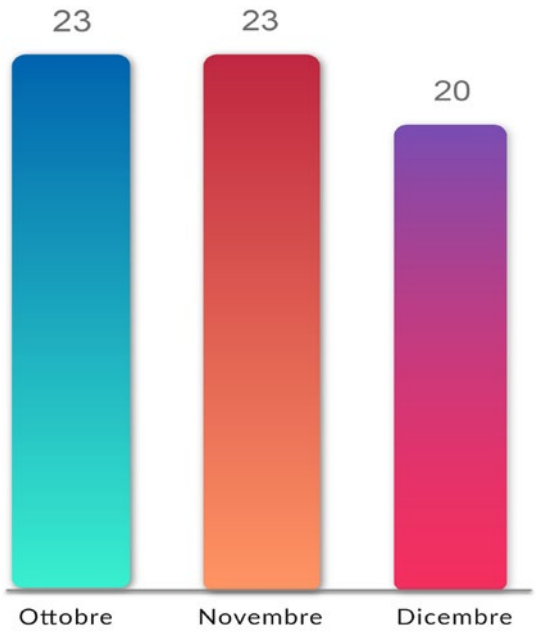
Di seguito riportiamo un'analisi dei settori e delle infrastrutture critiche colpite nel Q4 2022. In particolare, si evidenzia **una crescita** nel numero di attacchi ransomware rivolti ad infrastrutture critiche, dove continuano gli attacchi verso **infrastrutture scolastiche** da parte della **gang Vicesociety** e spiccano gli attacchi verso **infrastrutture sanitarie** da parte della **gang Royal,** che nell'ultimo trimestre si è distinta per numero di vittime.

Swascan
TINEXTA GROUP

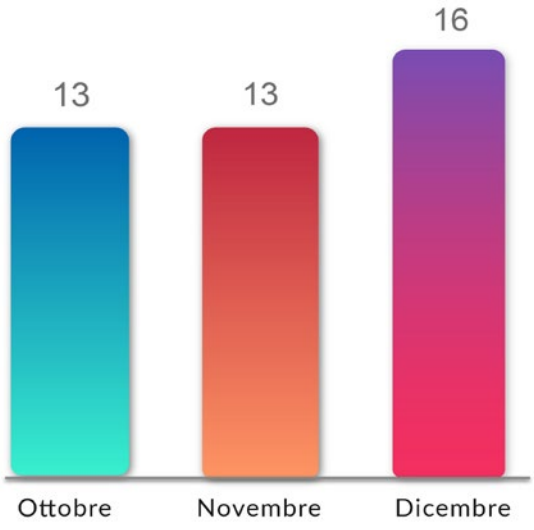
Attacchi per settore in percentuale- Q4 2022



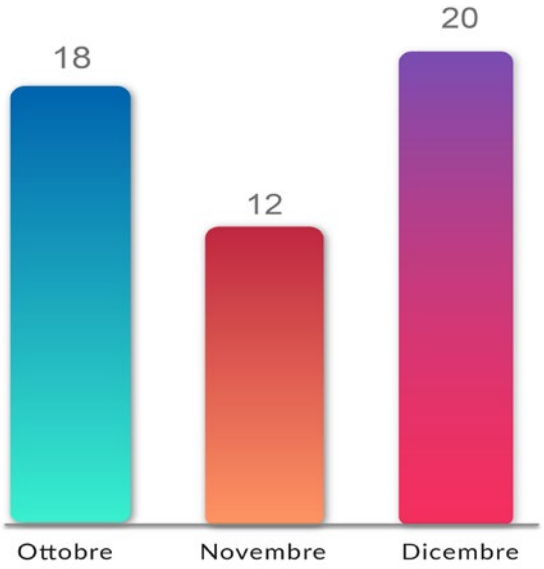
Attacchi Ransomware a Strutture Sanitarie



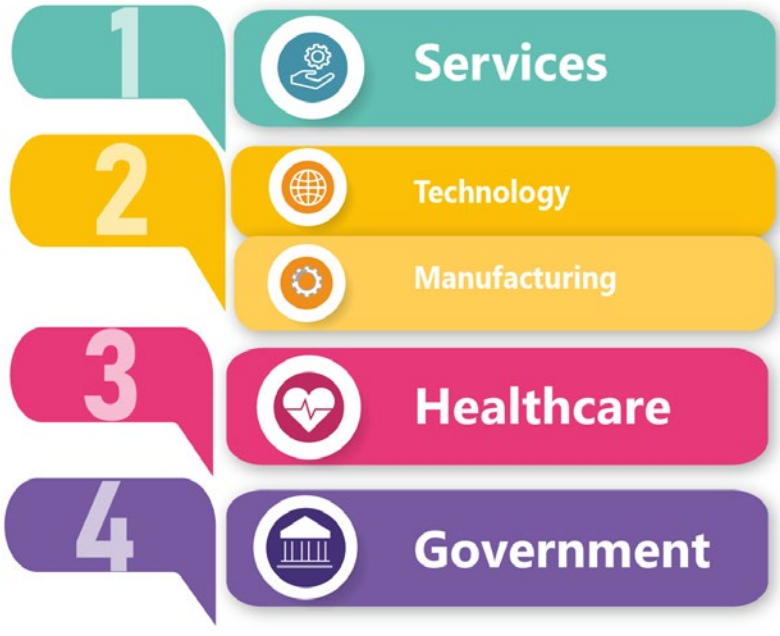
Attacchi Ransomware ad Amministrazioni Statali e Comunali



Attacchi Ransomware a Distretti Scolastici e Universitari



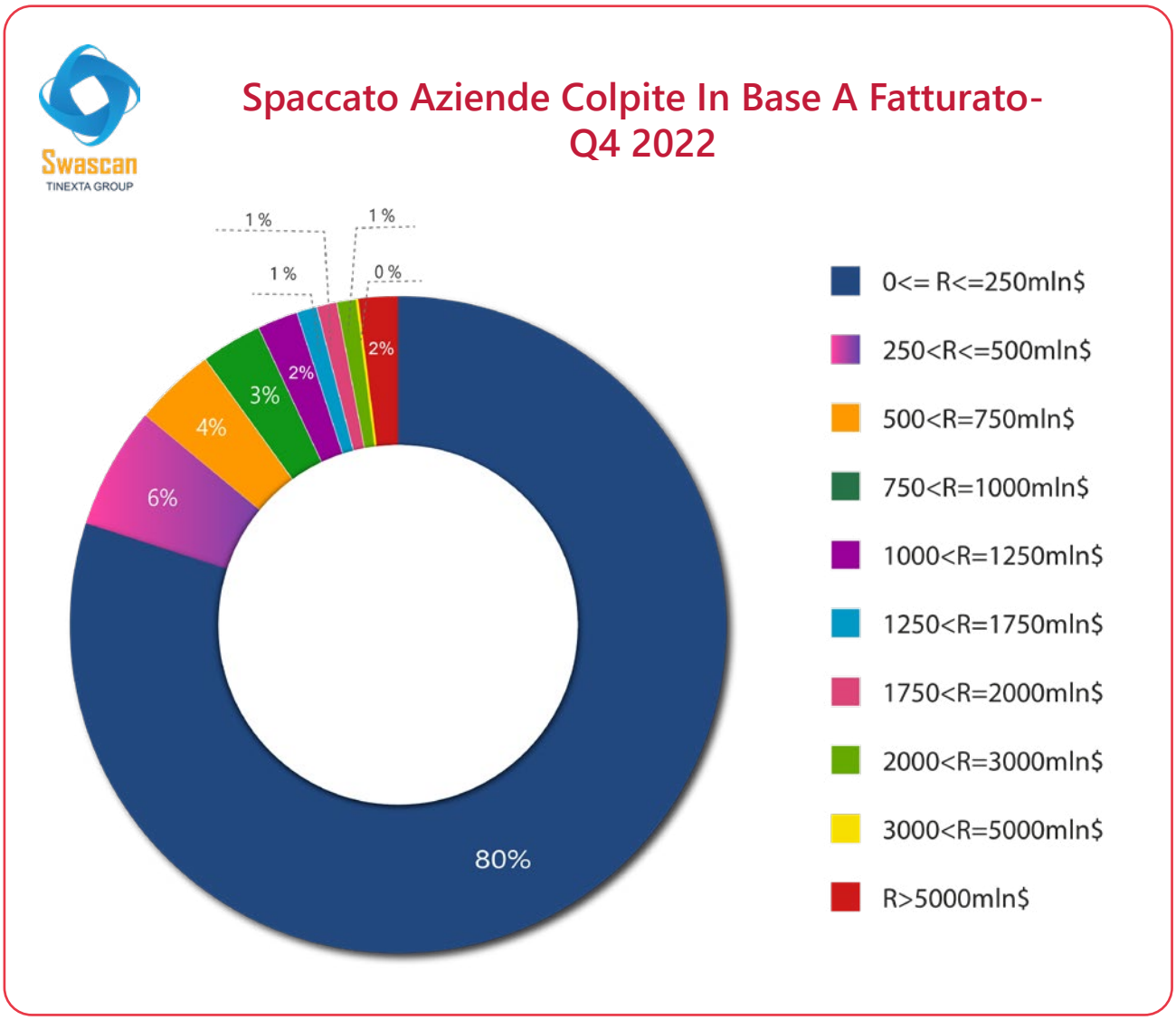
I Settori più Colpiti



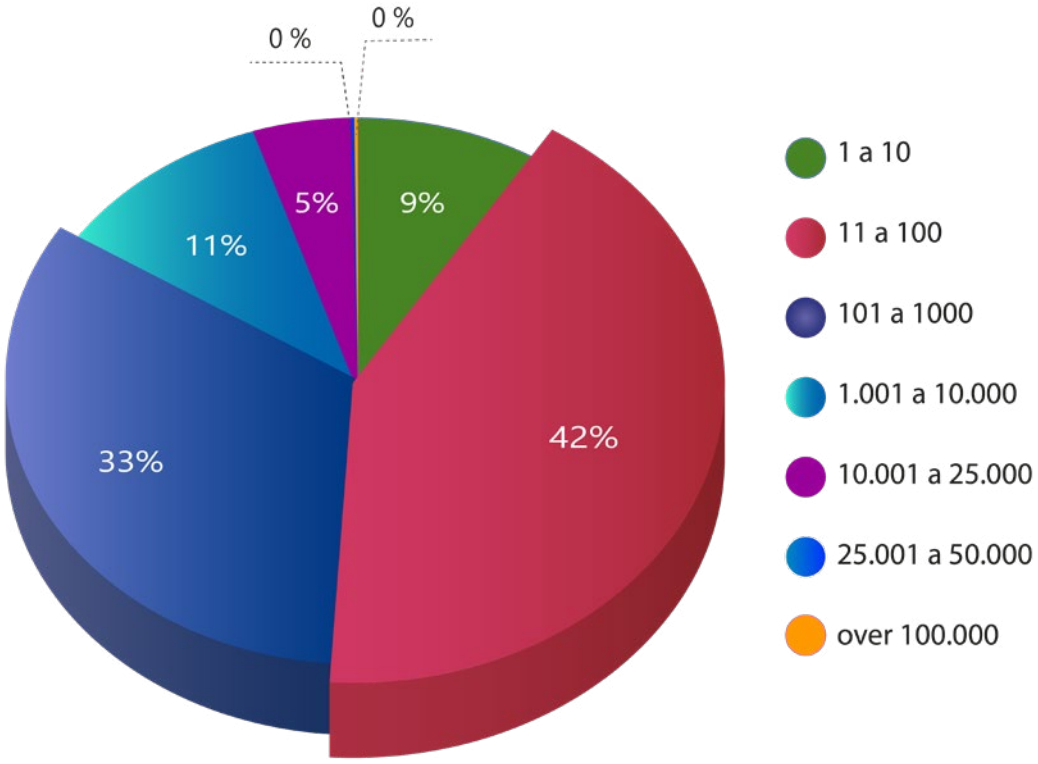
CLUSTER FATTURATO E DIPENDENTI AZIENDE VITTIME PUBBLICATE A LIVELLO GLOBALE

Le statistiche confermano che se l'anno scorso erano in aumento gli attacchi ransomware contro le grandi organizzazioni, **nel 2022** le azioni si sono intensificate notevolmente verso le **PMI,** considerate soggetti **più vulnerabili** in quanto spesso meno attrezzate a fronteggiare le minacce informatiche.

L'analisi è stata condotta scegliendo a campione **10 aziende vittime** per ognuna delle **10 gang ransomware** che si sono distinte nel periodo intercorso tra ottobre e dicembre 2022, per un totale di **100 aziende analizzate**. I dati sono poi stati aggregati in base al fatturato e al numero di dipendenti delle vittime:



Numero Dipendenti Aziende Colpite - Q4 2022



Riportiamo infine, una panoramica confrontando l'inizio e la fine del 2022 in termini di attacchi ransomware:

	Q1	Q2	Q3	Q4
Vittime di Data Leaks	544	707	700	753
Gruppi di ransomware totali	35	31	36	41
Vittime di LockBit	220	214	234	149
Paese più colpito	United States	United States	United States	United States
Totale Paesi colpiti	83	62	76	77
I 5 paesi più colpiti	United States, United Kingdom, Italy, Germany, Canada	United States, Germany, Canada, Italy, United Kingdom	United States, France, Spain, United Kingdom, Germany	United States, United Kingdom, Canada, Germany, Brasil
Settori più colpiti	Manufacturing	Services	Services	Services
PMI colpite	78%	85%	82%	84%

CONCLUSIONI

Cresce il numero delle imprese vittime di ransomware rispetto ad inizio anno: sono **753** gli obiettivi attaccati in **77 Paesi** nel quarto trimestre del 2022. Si tratta di un dato in **crescita del 38%** rispetto al Q1 2022, ma in calo del 23% rispetto al medesimo periodo del 2021. Un totale di **2704 vittime** nel corso dell'intero anno, 817 delle quali ad opera della **gang LockBit.**

Il panorama degli attacchi è cambiato in modo significativo nel corso dell'anno: se LockBit è rimasto di gran lunga il gruppo leader in termini di aziende colpite, abbiamo assistito al ritorno di Revil, uno dei gruppi più pericolosi al mondo e alla (definitiva?) uscita di scena di Conti: con un totale di 180 milioni di dollari di estorsioni dalle sue vittime nel 2021, la gang Conti era considerata una delle più pericolose almeno fino all'inizio del conflitto tra Russia e Ucraina quando, schierandosi apertamente verso posizioni pro-Putin, ha subìto conseguenti leak riguardanti la sua attività criminale.

Allo stesso tempo si è riscontrata l'ascesa di una moltitudine di nuovi gruppi concorrenti – Donut Leaks, DAIXIN, PLAY, Yanluowang, BianLian, IndustrialSpy e molti altri tra cui Black Basta, che non ha perso tempo ad emergere come una delle gang ransomware più pericolose del 2022. Individuato per la prima volta ad aprile, in soli 3 mesi aveva colpito 90 organizzazioni di alto profilo in tutto il mondo. La maggior parte di queste organizzazioni ha sede negli Stati Uniti, mentre un numero significativo si trova in Germania.

BlackBasta potrebbe essere un rebranding proprio della gang ransomware Conti: la tempistica della comparsa di BlackBasta è infatti immediatamente successiva alla chiusura delle operazioni di Conti.

Anche **Royal** si aggiudica la medaglia di una delle principali minacce del 2022. Emersa a gennaio 2022, la gang Royal ha intensificato in modo allarmante la propria attività negli ultimi mesi prendendo di mira organizzazioni sanitarie, in particolare negli Stati Uniti, con richieste di riscatto che variano da 250 mila a 2 milioni di dollari.

Nel terzo trimestre 2022 abbiamo riscontrato come l'aumento del numero di gang non fosse proporzionale all'aumento del numero di data leak pubblicati: questo porta dunque ad ipotizzare ad una crescita nel numero di vittime che hanno pagato il riscatto nel corso dell'ultimo anno, i cui dati non vengono pertanto pubblicati sui siti dei threat actors.

Aprile 2022 è stato il mese con il più alto numero di vittime, in cui la gang ransomware Stormous ha annunciato nel proprio leak site di aver fatto irruzione nei server di una nota azienda del settore food and beverages e aver rubato 161 GB, attaccata per il semplice motivo di essere stata l'azienda più votata a seguito di un sondaggio realizzato dalla gang stessa su Telegram.

Nello stesso mese un tech giant giapponese ha confermato che le sue attività canadesi sono state colpite da un attacco informatico, a meno di sei mesi dall'ultima volta che l'azienda è stata vittima di una violazione. Dietro l'attacco c'era **la gang Conti**, che ha dichiarato di aver rubato oltre 2.8 GB di dati.

Successivamente nel corso dell'anno, un famoso system integrator statunitense ha confermato che la sua rete aziendale è stata violata dal gruppo ransomware Yanluowang a Maggio. I threat actors hanno tentato di estorcere denaro minacciando di far trapelare le informazioni che avevano esfiltrato: l'azienda ha sempre negato che fossero state rubate informazioni sensibili, ipotesi poi confermata a seguito della pubblicazione dei dati sul sito della **gang Yanluowang.**

A giugno un attacco al comune di Palermo è stato rivendicato dalla **gang Vice Society,** causando interruzioni di servizio su larga scala. La banda criminale ha pubblicato i dettagli dell'attacco sul proprio sito di leak, rivelando che avrebbe diffuso i dati rubati se non fosse stato pagato un riscatto, ma senza condividere alcun campione di dati. Nello stesso mese, sempre in Italia, **BlackCat** ha chiesto all'Università di Pisa un riscatto di ben 4,5 milioni di euro per evitare la pubblicazione di dati trafugati dalla gang e relativi all'Università stessa: tuttavia, i threat actors ha pubblicato i dati sul proprio sito.

Sempre in riferimento all'Italia, a luglio la gang **LockBit** ha dichiarato di aver rubato 78 GB di dati a un Ente statale italiano (poi rivelatasi essere una piccola attività non legata alla PA italiana), mentre a novembre una società italiana specializzata nella produzione di impianti a gas auto GPL o metano, è stata vittima di un attacco informatico condotto da Hive. In un'e-mail ricevuta dall'azienda, i threat actors hanno affermato di essersi infiltrati nella loro rete dove sono rimasti per undici giorni, accedendo a file e documenti prima di criptare i loro server. I dati sono stati pubblicati sul sito della gang.

A dicembre l'ennesima azienda ospedaliera colpita. **Ragnar Locker** ha rivendicato la responsabilità dello stesso e ha già fatto trapelare 37 GB di dati rubati, sostenendo che si tratti solo del 5% del volume totale di dati esfiltrati.

Questa è solo una piccola parte delle aziende e delle infrastrutture critiche colpite nel corso dell'anno 2022, un anno durante il quale è stato inoltre rilasciato il codice sorgente di LockBit. La pubblicazione del codice di **LockBit 3.0** a settembre 2022, apre difatti le porte ad uno scenario con nuove gang nate dai leak dei codici sorgente di organizzazioni di criminali informatici: questo spiegherebbe anche **l'aumento del 17%** nel numero di gang da inizio anno. Il builder di LockBit 3.0 consente di fatto a chiunque di costruire proprie versioni del ransomware: questo è ciò che è accaduto col gruppo di criminali informatici "**Bl00Dy**", una gang in azione da fine settembre 2022 con un proprio ransomware derivato proprio da Lockbit. Assistiamo quindi ad un continuo proliferare di new entry nel mondo delle gang ransomware.

Inoltre sviluppare, mantenere e aggiornare i ransomware richiede tempo, competenze e soprattutto investimenti. Una mole di risorse necessarie che difficilmente trovano un riscontro rispetto al numero dei nuovi prodotti e relativi attori malevoli apparsi negli ultimi mesi.

Qualche anno fa, in caso di attacco ransomware, non era difficile puntare il dito sui "soliti noti". Oggi non è insolito imbattersi in nuovi attori o collettivi che mutano con cadenza settimanale. Sono cadute le barriere di ingresso, il fenomeno si è democratizzato grazie **all'effetto "idra"**: dalle gang che chiudono l'attività volutamente **(come Conti)** o forzate dalle forze dell'ordine **(come Hive)** o che hanno subito un data leak del codice e che quindi lo "diffondono" involontariamente online **(come Babuk)**, ne sorgono molte altre.

Nuove entità forti delle competenze ed esperienze dei "disoccupati" oppure nuove entità alle prime armi che "pescano" direttamente **il know how** (il codice) dai vari forum dedicati al Criminal Hacking. Per non menzionare il nuovo trend di vendita nel darkweb di soluzioni as a service.

Nel complesso, si è registrato un declino di attacchi nel mese di agosto 2022. **L'industria dei servizi** risulta essere **il settore più colpito** e gli Stati Uniti continuano ad essere il paese più attaccato (fatto dovuto al gran numero di potenziali vittime presenti). In diminuzione invece il trend del numero di vittime pubblicate in Europa ed in particolar modo in Italia: se nel primo trimestre il Bel Paese si posizionava al terzo posto con un totale di 40 aziende colpite, i cui dati sono stati pubblicati, a fine anno si contano "solo" 14 vittime, scendendo così al 10° posto.

Dall'analisi è emerso come **l'80%** del campione delle aziende con dati pubblicati abbia un fatturato che non superi i 250 milioni di dollari.

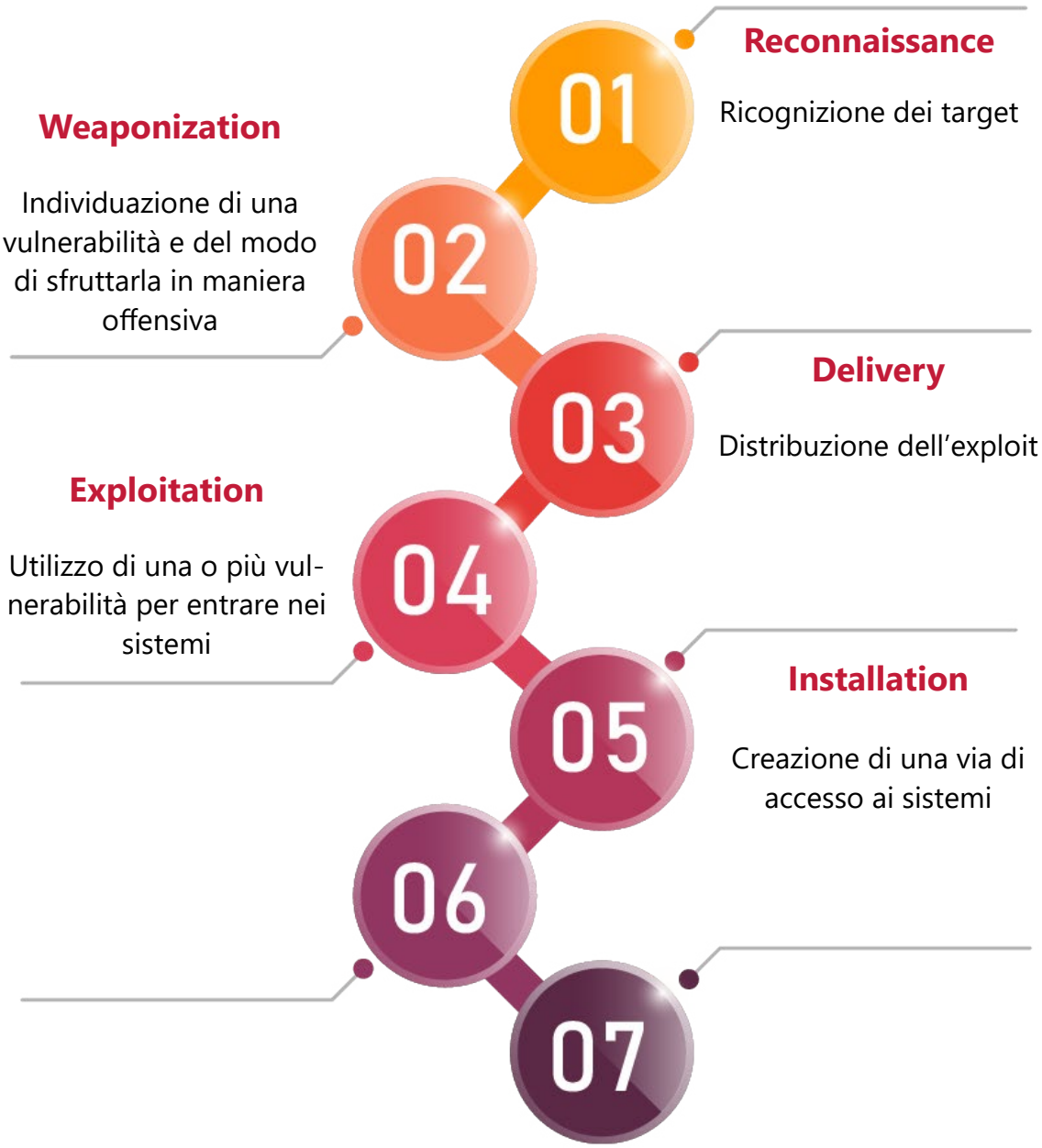
Inoltre l'**84%** delle stesse aziende ha un numero di dipendenti inferiore a 1000, dato che conferma un incremento del numero di attacchi verso le Piccole Medie Imprese e che sottolinea una grande differenza rispetto all'anno precedente, dove la tendenza era verso organizzazioni "più grandi" che, pur avendo una maggiore disponibilità economica, implementano allo stesso tempo strutturate misure di sicurezza informatica. Questo evidenzia l'importanza di soluzioni di cybersecurity e mostra come ad oggi le aziende di piccole dimensioni siano più inclini al pagamento del riscatto, comunque proporzionale al fatturato dell'azienda stessa.

L'attenzione delle gang ransomware nei confronti della PMI italiana può essere sicuramente attribuibile alla maggiore facilità nel colpire questo settore. Spesso budget a disposizione non adeguati, minori competenze disponibili e una minore sensibilizzazione del personale sono e rappresentano una opportunità per i criminal hacker. A questo dobbiamo aggiungere che spesso sono proprio queste aziende che cedono al ricatto poiché i sistemi di backup (ultima possibilità per il recupero dei dati) non sono configurati in sicurezza e di conseguenza vengono anch'essi crittografati. Diventano così completamente inermi e spesso il pagamento del ricatto diventa l'unica via per poter riprendere l'operatività del business. Ecco che se da un lato sono un target più facilmente aggredibile sono anche un target che garantisce una maggiore probabilità di guadagno.

La PMI non ha un ruolo solo economico nel breve termine per queste gang. La PMI italiana rappresenta una grossa fetta del prodotto interno lordo, è il nostro vantaggio competitivo italiano. Il loro know-how, i loro brevetti, i loro progetti, in ogni attacco informatico da ransomware, sono anche informazioni che vengono esfiltrate. Dati e informazioni nell'attuale conflitto potrebbero essere anche interessanti per una Russia che ha l'import completamente bloccato. Ecco un ulteriore elemento di attenzione e preoccupazione nazionale. La perdita di questi dati rappresenta a tutti gli effetti un danno competitivo a livello geopolitico nel medio e lungo termine.

Sicuramente è necessario intervenire con aiuti concreti alla PMI, il PNRR potrebbe essere la soluzione ma allo stesso tempo è necessario intervenire legalmente sulla questione del pagamento dei riscatti. Di fatto diventerebbe uno scudo di tutela per le nostre aziende poiché andrebbe a disincentivare gli attacchi legati al cyber crime riducendo drasticamente la possibilità di ottenere un guadagno dagli attacchi informatici.

COME OPERA IL RANSOMWARE: CYBER KILL CHAIN



LE MODALITÀ DI ATTACCO

Le principali modalità di attacco che potrebbero essere messe in campo contro le infrastrutture critiche sono le seguenti:

1) Social Engineering: Nel contesto della sicurezza informatica, il social engineering è l'uso dell'inganno per manipolare le persone nel divulgare informazioni riservate o personali che possono essere utilizzate a fini fraudolenti. In altre parole, le persone possono essere ingannate nel condividere informazioni che altrimenti non divulgherebbero. La variante più comune è il Phishing, mail costruite ad hoc per ingannare il destinatario e costringerlo a rivelare dati o informazioni sensibili;

2) Botnet: Le botnet sono grandi reti di computer compromessi, la cui potenza di elaborazione viene utilizzata all'insaputa dell'utente per svolgere attività criminali. Questo può includere la distribuzione di spam o e-mail di phishing, così come l'esecuzione di attacchi DDoS, ma anche il furto di credenziali di accesso a servizi aziendali e non solo;

3) Sfruttamento Vulnerabilità: In cybersecurity, una vulnerabilità è una criticità che può essere sfruttata dai Criminal Hacker per ottenere un accesso non autorizzato a un sistema informatico. Dopo aver sfruttato una vulnerabilità, un criminale informatico può eseguire codice dannoso, installare malware e persino rubare dati sensibili;

4) Supply Chain attack: Ogni azienda o infrastruttura non è più oramai monolitica, ma si appoggia su una lunga e complessa supply chain digitale. I Criminal Hacker possono colpire il proprio target proprio andando a compromettere un fornitore a monte;

5) 0 – Day: Questa è l'insidia maggiore per ogni organizzazione, gli zero-day sono così noti perché lasciano appunto – zero giorni di tempo – agli sviluppatori per correggere una vulnerabilità prima che venga sfruttata. In essenza sono criticità che vengono scoperte solo nel momento in cui un attacco è già in corso.

COME DIFENDERSI DAL RANSOMWARE: IL CYBER SECURITY FRAMEWORK

L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno consolidati e rispettati i tre canoni di:

- **Sicurezza Predittiva**
- **Sicurezza Preventiva**
- **Sicurezza Proattiva**

Swascan
TINEXTA GROUP

Sicurezza Predittiva

1. Identifica le minacce Cyber fuori dal perimetro aziendale operando a livello di web, Darkweb e Deepweb
2. Ricerca eventuali minacce emergenti
3. Effettua attività di Early Warning
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di attenzione alla Sicurezza Proattiva

Sicurezza Proattiva

1. Identifica le minacce cyber che operano nel perimetro aziendale
2. Contrasta e blocca gli attacchi informatici
3. Gestisce i Cyber Incident
4. Fornisce le evidenze alla Sicurezza Preventiva
5. Indica le aree di investigazione alla Sicurezza Predittiva

Sicurezza Preventiva

1. Verifica e misura il Rischio Cyber
2. Definisce i piani di remediation
3. Indica il Rischio esposto al Layer di Sicurezza Proattiva
4. Fornisce le aree di Investigazione alla Sicurezza Predittiva

Sicurezza Predittiva

Domain Threat Intelligence: La Domain Threat Intelligence ricerca le informazioni pubbliche e semipubbliche relative alle vulnerabilità del dominio, sottodomini ed email compromesse. Il servizio non effettua alcun test sul target. Opera unicamente sulle informazioni disponibili sul web, Darkweb e Deepweb. Raccoglie, analizza e clusterizza le informazioni disponibili a livello OSINT (Open Source Intelligence) e Closint (Close Source Intelligence) presenti su database, forum, chat, newsgroup.
Nello specifico, in base al dominio-target di analisi, identifica:

- Potenziali Vulnerabilità
- Dettagli delle Vulnerabilità in termini di CVE, impatti e severity
- Impatti GDPR (CIA)
- Numero dei Sottodomini
- Numero Potenziali e-mail compromesse (vengono solo conteggiate e non raccolte o trattate)
- Numero delle Source delle e-mail compromesse
- Typosquatting

Cyber Threat Intelligence: È il servizio evoluto di Threat Intelligence di Swascan. Effettua una attività di ricerca, analisi e raccolta delle informazioni presenti a livello web, Darkweb e Deepweb relativamente al dominio/target di analisi.
Nello specifico:

- Data Leaks: credenziali/source/data
- Identifica Forum/Chat ...
- Botnet relative a dispositive di Clienti, Fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

Early Warning Threat Intelligence: È il servizio di Early Warning che segnala giornalmente le evidenze che vengono identificate e raccolte nel Darkweb e Deepweb relativamente al target di analisi.
Nello specifico:

- Data Leaks
- Scraping data
- Phishing data
- Botnet

Sicurezza Preventiva

Tecnologico

Vulnerability Assessment: Esegue la scansione di siti e applicazioni web per identificare e analizzare in modo proattivo le vulnerabilità di sicurezza.

Penetration Test: Le attività di Penetration Test sono svolte da Penetration Tester certificati e in linea con gli standard internazionali OWASP, PTES e OSSTMM.

Human Risk

Phishing/Smishing attack Simulation: Permette alle aziende di prevenire i danni dovuti ad attacchi di phishing/smishing attraverso delle vere e proprie simulazioni di attacco. È infatti possibile, attraverso un'interfaccia web, inviare vere e proprie campagne di phishing/ smishing simulate che generano delle insostituibili occasioni di apprendimento per i dipendenti. I dipendenti, infatti, grazie a questi attacchi simulati riusciranno, in futuro, ad individuare una vera e-mail di phishing o un messaggio di smishing e ad evitarla. Un'insostituibile attività di formazione e awareness dei tuoi dipendenti tramite vere e proprie simulazioni di attacco phishing/smishing .

Awareness: Corsi di formazione dedicati di Cybersecurity in aula o tramite Webinar. Attività di Awareness per il personale tecnico, per i dipendenti e per i Top Manager.

Processo – Compliance

ISO27001: ISO/IEC 27001:2013 (ISO 27001) è lo standard internazionale che descrive le best practice per un ISMS (sistema di gestione della sicurezza delle informazioni, anche detto SGSI, in italiano). Dal momento che l'informazione è un bene che aggiunge valore all'organizzazione e che ormai, la maggior parte delle informazioni, sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

ICT Security Assessment: L'ICT Security Assessment è una metodologia proprietaria di Swascan che permette alle aziende di verificare e misurare il proprio livello di rischio cyber e di valutare l'efficacia delle misure di sicurezza adottate. Il servizio fornisce le indicazioni e le azioni correttive da adottare a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.

Sicurezza Proattiva

SOCaaS: La progettazione, la messa in esercizio e il mantenimento di un Security Operation Center può essere costoso e complesso. Il servizio **SOC as a Service** Swascan è la soluzione più efficace, efficiente, coerente e sostenibile per i contesti aziendali. Il Soc as a Service, con il suo servizio di Monitoring & Early Warning, permette di **identificare**, **rilevare, analizzare** e segnalare gli attacchi cyber prima che possano trasformarsi in una minaccia concreta per l'azienda.
Un team dedicato all'attività di **Monitoring & Early Warning,** reattivo delle minacce informatiche sulle reti locali, ambienti cloud, applicazioni ed endpoint aziendali. Il nostro team di Security Analyst monitora i dati e le risorse ovunque risiedano all'interno dell'azienda. Indipendentemente dal fatto che le risorse siano archiviate nel cloud, in locale o in entrambi. L'attività di monitoring e segnalazione permette di agire solo quando viene identificata una minaccia reale.

Incident Response Management: è un insieme di risorse e procedure organizzate e strutturate per garantire la corretta reaction e gestione degli incidenti informatici. In caso di incidente informatico, Data Breach, DDoS, attacco Ransomware e/o relativo Data Recovery è necessario affrontare e rispondere con un approccio strutturato, predisposto e organizzato per affrontare in maniera efficace ed efficiente la violazione della sicurezza e per ridurre gli impatti a livello di Business Continuity aziendale. L'obiettivo dell'Incident Response è quello di:

- Gestire l'incidente.
- Limitare i danni diretti e indiretti.
- Ridurre tempi e costi di ripristino.

DISCLAIMER

In questa analisi quando vengono menzionate le numeriche inerenti alle vittime, sono state prese in considerazione unicamente quelle entità che non solo hanno subito un attacco ransomware, ma si sono viste anche vittime di Data Leak tramite double extortion.

ABOUT US

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan srl è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di idetità digitale e sicurezza digitale.

Analysis by:

Martina Fonzo
Riccardo Michetti

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI