Swascan
TINEXTA GROUP

Threatland Report cyber security Q1:

Dal Ransomware Al phishing, tutti i trend del 2023

www.swascan.com
info@swascan.com

SOMMARIO

Cyber risk summary ..... Pg. 03

Phishing ..... Pg. 05

Malware ..... Pg. 09

- Elementi importanti dell'analisi ..... Pg. 10
- Mirai ..... Pg. 11
- Hajime ..... Pg. 11

CVE trend ..... Pg. 13

La minaccia ransomware ..... Pg. 15

- Il contesto ..... Pg. 16
- Le gang più attive nel Q1 2023 ..... Pg. 19
- Distribuzione geografica globale delle vittime ..... Pg. 22
- I settori presi di mira dalla minaccia ransomware ..... Pg. 26
- Cluster vittime in base a personale e fatturato ..... Pg. 29
- Le aziende colpite in base al fatturato ..... Pg. 29

Conclusioni ..... Pg. 32

- Previsioni Q2 2023 ..... Pg. 34
- Il commento del CEO di Swascan, Pierguido Iezzi ..... Pg. 35

Come difendersi dal Ransomware: Il Cyber Security Framework ..... Pg. 36

Disclaimer ..... Pg. 37

About us ..... Pg. 38

CYBER RISK SUMMARY

Il primo trimestre del 2023 ha visto un aumento significativo di attacchi informatici mirati al furto di dati e alla richiesta di riscatti in cambio del ripristino dei sistemi colpiti.

- **898 obiettivi attaccati tramite ransomware in 79 paesi diversi nel primo trimestre del 2023, con una crescita del 19% rispetto al trimestre precedente.**
- **+161% di vittime di ransomware tra il mese di gennaio 2023 e marzo 2023.**
- **Aumento delle vittime rispetto al Q4 2022 del 19%.**
- **Aumento di vittime in Italia rispetto al Q4 2022 dell'85.7%.**
- **Facebook, Office365 i due nomi più ricorrenti usati dai Criminal Hacker nelle campagne di phishing.**
- **Hajime e Mirai i due malware che hanno fatto registrare i picchi di attività più elevanti nel primo trimestre del 2023.**
- **Rischio Supply chain in aumento anche per la grave vulnerabilità sui sistemi 3CX**

Il SOC e Threat Intelligence Team di Swascan ha condotto un'analisi approfondita sugli scenari ransomware, fornendo un quadro dettagliato delle minacce emergenti e delle tendenze in evoluzione.

In particolare, le gang ransomware hanno riconfermato la loro posizione di minaccia predominante nel panorama cyber, causando gravi danni economici e reputazionali a molte vittime.

In questo report, per meglio comprendere gli impatti e la portata del fenomeno, sono stati analizzati anche altri aspetti della cyber kill chain per restituire una fotografia più completa di come il ransomware va a impattare le organizzazioni.

La cyber kill chain – ovvero gli step che portano all'infezione ransomware – è universalmente riconosciuta come:

- **Ricognizione - compresa la raccolta di indirizzi e-mail delle vittime da prendere di mira**
- **Weaponization- accoppiamento di un exploit con una backdoor in un payload.**
- **Delivery - consegna del payload tramite e-mail, web e altri canali.**
- **Exploitation - sfruttamento di una vulnerabilità per eseguire codice dannoso sul sistema della vittima.**
- **Installazione - installazione di malware su un asset IT.**
- **Comando e controllo - apertura di canali di comunicazione per la manipolazione remota della vittima.**
- **Azioni sugli obiettivi - realizzazione di obiettivi originali con accesso remoto al sistema della vittima.**

Di seguito sono state sviscerate le fasi principali di questa catena, che si concretizzano, in particolare, tramite i vettori del phishing, malware e lo sfruttamento di vulnerabilità (anche note come CVE).

PHISHING

Il phishing è una tecnica utilizzata dagli Criminal hacker per rubare informazioni personali e finanziarie dalle vittime, ma anche nel consegnare il malware che da via all'infezione ransomware.

Il Q1 2023 è stato caratterizzato da una crescente minaccia degli attacchi di spear-phishing, Business E-mail Compromise (BEC) e E-mail Account Compromise (EAC), sfruttando tattiche di social engineering per ingannare i dipendenti delle aziende e ottenere accesso alle loro informazioni sensibili o installare malware. In particolare, gli attacchi BEC comportano spesso il reindirizzamento di fondi verso conti sotto il controllo dei criminal hackers, che sfruttano metodi relativamente come il typosquatting o lo spoofing di domini aziendali nelle intestazioni delle e-mail.

Il Q1 2023 è stato caratterizzato da una crescente minaccia degli attacchi di spear-phishing, Business E-mail Compromise (BEC) e E-mail Account Compromise (EAC), sfruttando tattiche di social engineering per ingannare i dipendenti delle aziende e ottenere accesso alle loro informazioni sensibili o installare malware. In particolare, gli attacchi BEC comportano spesso il reindirizzamento di fondi verso conti sotto il controllo dei criminal hackers, che sfruttano metodi relativamente come il typosquatting o lo spoofing di domini aziendali nelle intestazioni delle e-mail.

Nel Q1 2023, diverse aziende e servizi online sono stati bersaglio di campagne di phishing, con Facebook in testa alla lista con il 18% degli attacchi. Questi attacchi spesso sfruttano la popolarità del social network per convincere gli utenti ad inserire le loro credenziali di accesso in siti web contraffatti, con l'obiettivo di rubare le informazioni personali degli utenti.

Al secondo posto c'è Office365, con il 17% degli attacchi di phishing, seguito da Bet365, con l'11%. Questo sito web di scommesse sportive è stato spesso utilizzato come esca per convincere gli utenti ad inserire le loro informazioni di pagamento.

Al quarto posto c'è DHL con l'8%, spesso sfruttato dagli Criminal hacker per creare e-mail contraffatte che sembrano legittime, convincendo le vittime a fornire le loro informazioni personali.

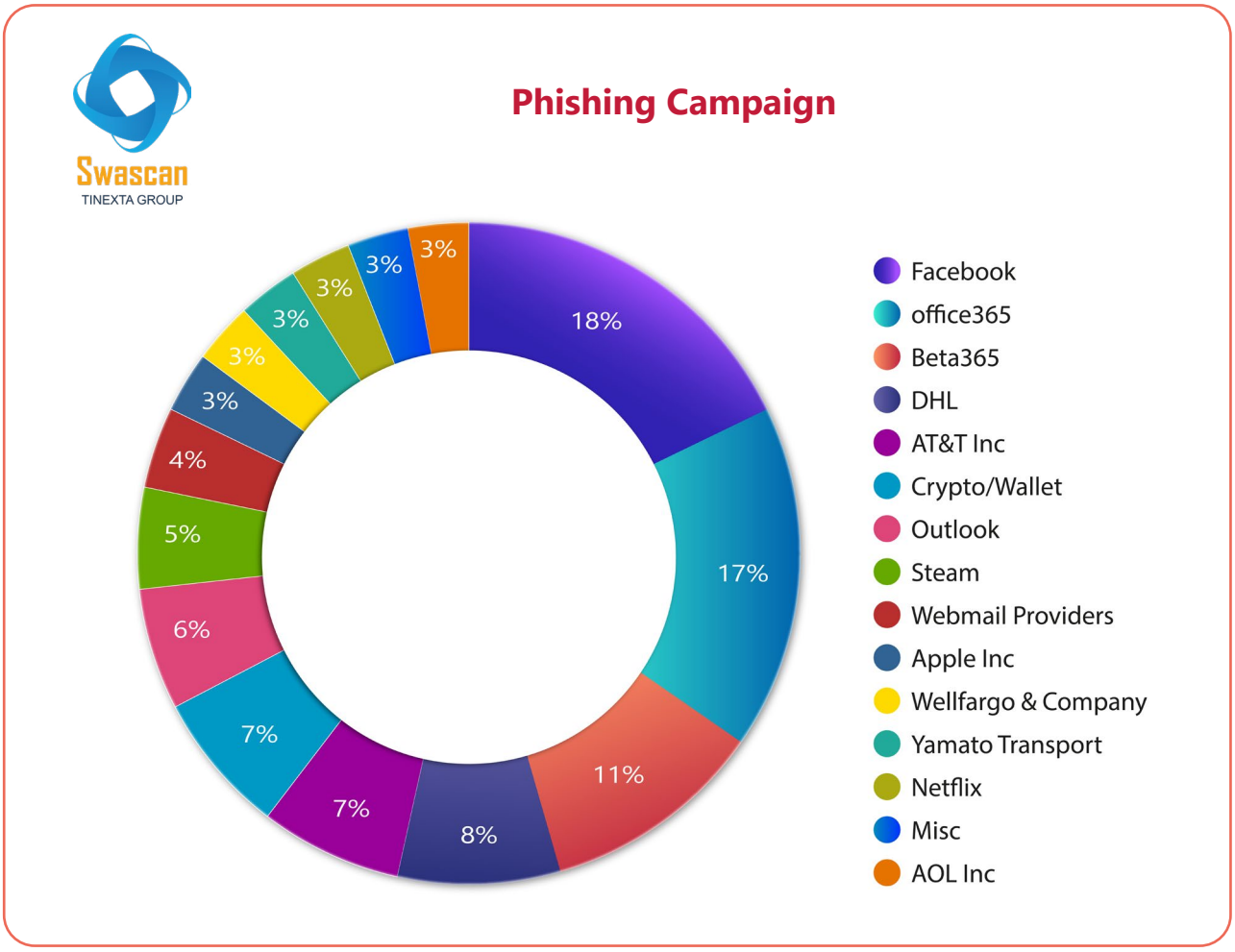
Il resto della lista include AT&T Inc. (7%), Crypto/Wallet (7%), Outlook (6%), Steam (5%), Webmail Providers (4%), Apple Inc. (3%), Wells Fargo & Company (3%), Yamato Transport (3%), AOL Inc. (3%), Netflix Inc. (3%) .

Aggregando i settori rileviamo che

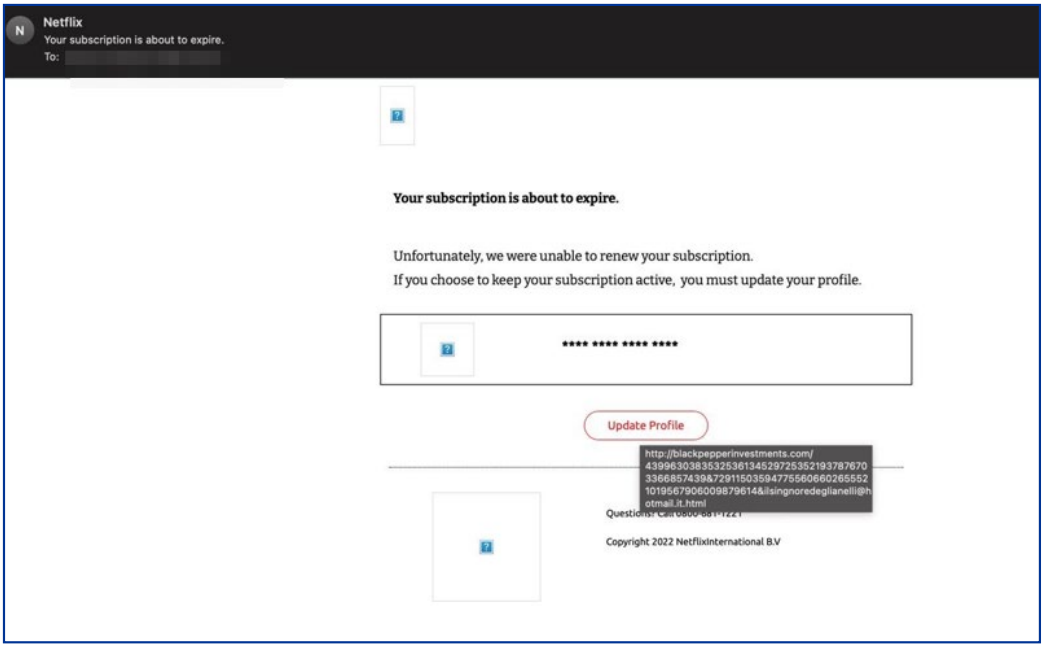
L'attenzione verso il mondo posta elettronica (pari al 30% degli attacchi phishing) è comprensibile perché avendo accesso ai sistemi di posta è possibile:

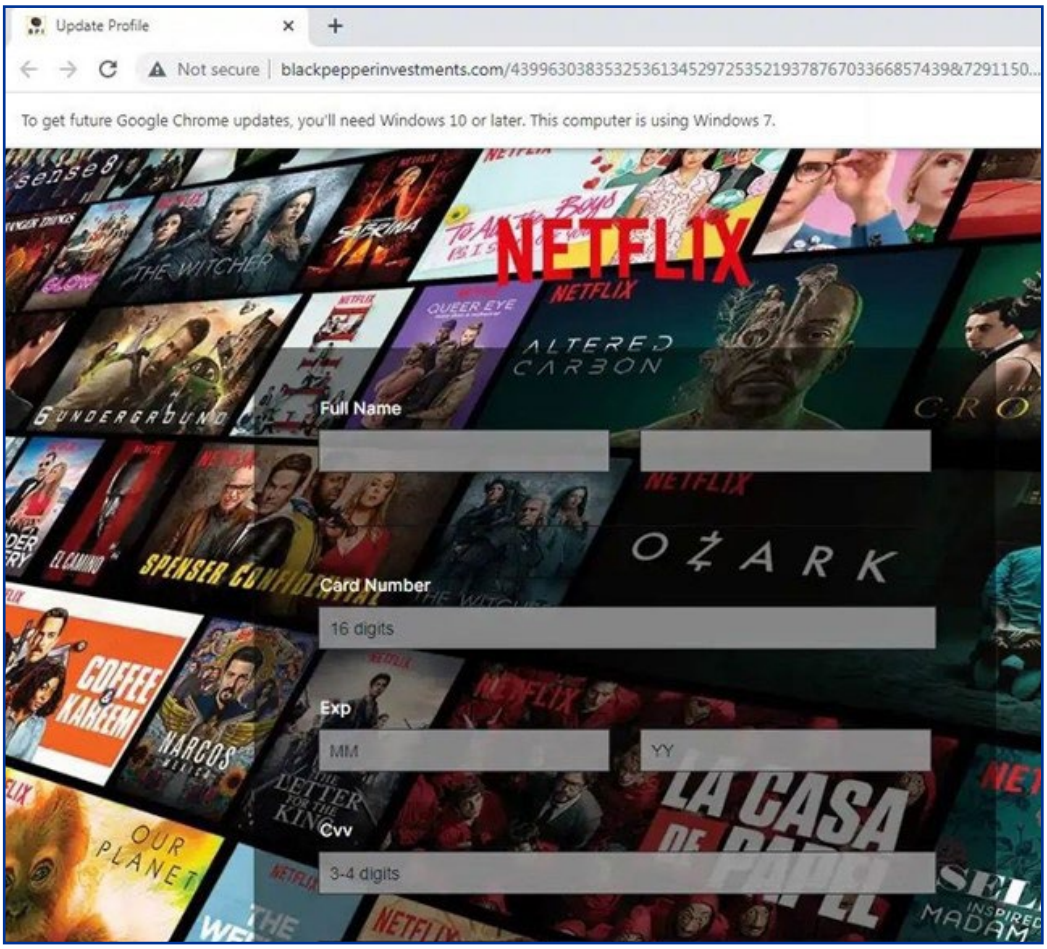
- Rubare credenziali
- Effettuare Frodi Informatiche (tipico nelle aziende il modello BEC)
- Usare la posta elettronica compromessa come vettore di attacco phishing verso contatti interni ed esterni

E' particolare l'attenzione verso il mondo dello shipping and delivery (pari al 14%) collegato al mondo dei colossi dell'e-commerce. Queste rende l'esca molto efficace



Di seguito riportiamo un esempio di campagna di Phishing:





Questa mail sembra essere un tentativo di phishing mirato a imitare Netflix. L'indirizzo del mittente, infatti, non è in alcun modo collegato al noto servizio di streaming video. Il link a cui si rimanda nella mail è http://blackpepperinvestments.com/ seguito da una serie di parametri e variabili in input alla URL.

Analizzando i dettagli di registrazione del dominio è possibile evidenziare che la data di creazione risalga al 29/09/2022:

RECORD	VALUE
Emails	abuse@godaddy.com
Name	Registration Private
Name Servers	NS05.DOMAINCONTROL.COM
Org	Domains By Proxy, LLC
Address	DomainsByProxy.com
Address	2155 E Warner Rd
City	Tempe
Country	US
Creation Date	2022-09-29T06:23:20
Creation Date	2022-09-29T01:23:20

La pagina web a cui il link conduce imita l'aspetto di Netflix, con il logo e la grafica simili; tuttavia, il form di inserimento mira ad esfiltrare nello specifico anche il numero CVV della carta di credito delle vittime dell'attacco informatico: quest'informazione renderebbe più fruibile l'utilizzo della carta di credito inserita da parte dei phishers.

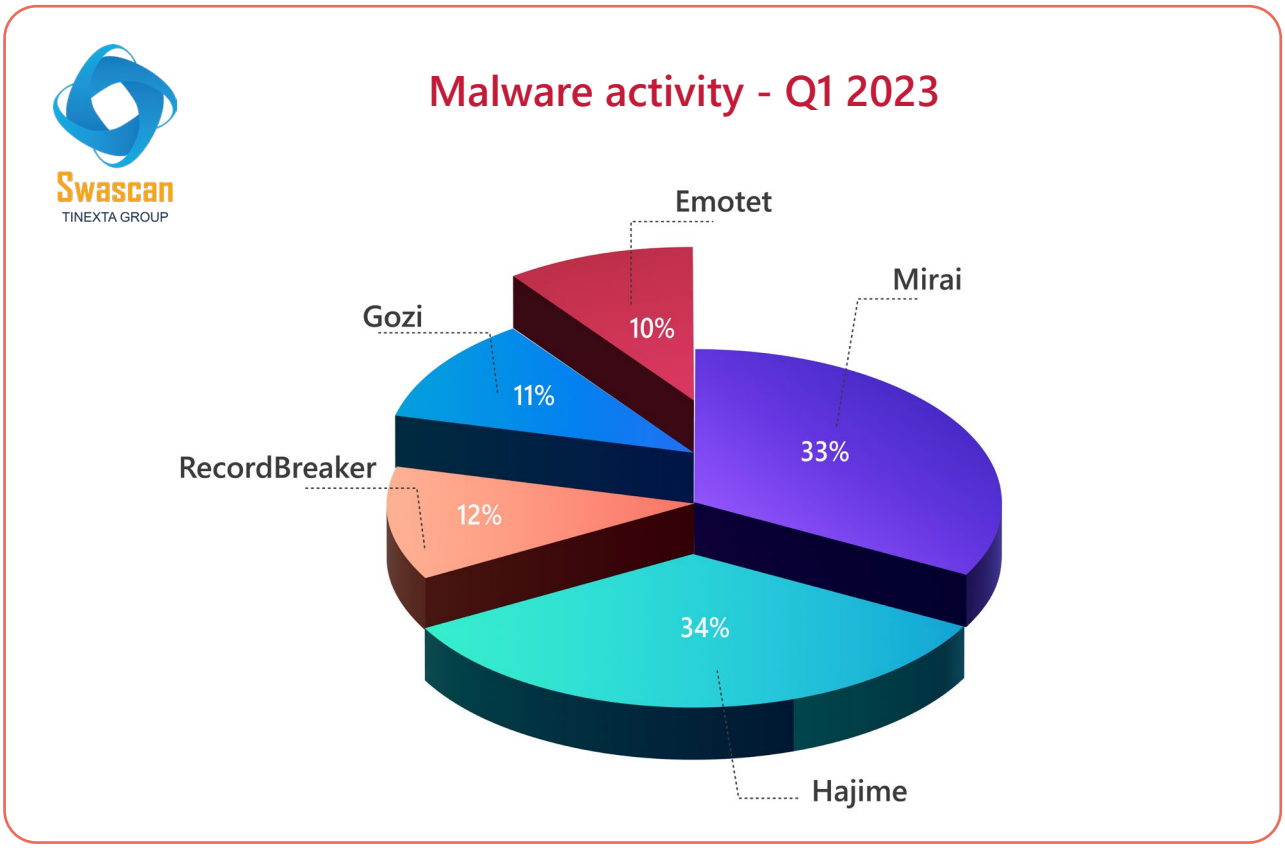
Il messaggio di posta elettronica cerca di creare un senso di urgenza, affermando che l'iscrizione dell'utente sta per scadere e che deve essere aggiornata per mantenerla attiva. Questo è un tipico stratagemma utilizzato dai truffatori per spingere le vittime ad agire in modo impulsivo e fornire informazioni personali.

In conclusione, questa mail sembra essere un tentativo di phishing volto ad imitare Netflix. È importante prestare attenzione a questi segnali di allarme e non fornire informazioni personali o finanziarie a siti web sospetti.

MALWARE

I malware possono essere utilizzati per supportare l'attacco di ransomware in diversi modi. Per esempio, i Criminal Hacker possono utilizzare malware come Trojan o spyware per entrare nei sistemi delle vittime e raccogliere informazioni preziose, come password o accessi di sistema, che poi possono essere utilizzate per lanciare attacchi di ransomware più mirati e dannosi.

Nel primo trimestre del 2023, i malware continuano a rappresentare una minaccia per la sicurezza informatica di aziende e individui in tutto il mondo. Il **SOC** & **Threat Intelligence Team di Swascan** ha identificato i malware più diffusi durante questo periodo: al primo posto **Hajime** e **Mirai,** che hanno rappresentato rispettivamente il **34% e il 33% degli attacchi.**



Mirai è un malware noto per essere stato utilizzato per attaccare dispositivi IoT in tutto il mondo, causando interruzioni di servizio e problemi di sicurezza. Hajime, invece, è un worm che si diffonde attraverso dispositivi IoT e che cerca di creare una rete botnet per attaccare altri sistemi: ha come obiettivo molti degli stessi dispositivi di Mirai, ma si differenzia notevolmente nella progettazione e nel funzionamento.

Al terzo posto della lista dei malware più diffusi si trova **RecordBreaker,** con il **12% degli attacchi.** Si tratta di un malware che utilizza tecniche avanzate di evasione per eludere le misure di sicurezza, rendendolo particolarmente difficile da rilevare. Si tratta del successore di Raccoon Stealer e viene spesso indicato come Raccoon Stealer 2.0. Dal 2019, il malware Raccoon è stato diffuso come un malware-as-a-service su diversi forum di criminalità informatica. Il gruppo Raccoon Stealer è stato sciolto nel marzo 2022 a causa della morte di uno dei suoi sviluppatori nella guerra tra Ucraina e Russia. Tuttavia, nel giugno 2022, è stata individuata una nuova versione di Raccoon Stealer, inizialmente chiamata "Recordbreaker", identificata in seguito come una versione aggiornata del malware Raccoon Stealer.

Al quarto posto si trova **Gozi**, con l'**11% degli attacchi.** Si tratta di un trojan bancario che esfiltra le credenziali di accesso ai conti bancari online degli utenti, causando danni finanziari.

Infine, al quinto posto della lista si trova **Emotet**, con il **10% degli attacchi.** Questo malware si diffonde principalmente attraverso e-mail di spam che contengono collegamenti o documenti dannosi.

In sintesi, il primo trimestre del 2023 ha visto una diffusione significativa di malware noti per la loro pericolosità e capacità di eludere le misure di sicurezza. Di seguito un'analisi nel dettaglio dei 5 malware che si sono distinti nel Q1 2023.

ELEMENTI IMPORTANTI DELL'ANALISI

- Rilevamento di security monitoring tools da parte di Mirai Botnet.
- Operazione SNQUERY effettuata da parte di Mirai Botnet.
- Correlazione tra il sample di Mirai con il malcoder username zxcr9999.
- Utilizzo del processore ARM Cortex-A5 da parte di Hajime.
- Esecuzione di funzioni SVC da parte di Hajime.
- Assembly details e assembly name particolari del threat Gozi.
- Exports calling da parte di Emotet.
- Utilizzo di Windows 7 samples e la libreria MTGestures da parte di Emotet.
- Enumerazione di diverse informazioni e risorse da parte di RecordBreaker.
- Somiglianze di alcuni dettagli ed attributi (come, ad esempio, assembly details ed assembly names) tra RecordBreaker e Gozi.

MIRAI

Read More

HAJIME

Read More

CVE TREND

- **Gli exploit CVE (Common Vulnerabilities and Exposures) sono vulnerabilità di sicurezza note che possono essere sfruttate da un attaccante per violare un sistema informatico. I ransomware, come molte altre forme di malware, spesso sfruttano queste vulnerabilità per diffondersi e infettare nuovi sistemi.**
- **In particolare, gli attaccanti possono utilizzare exploit CVE per ottenere l'accesso ai sistemi vulnerabili e installare il ransomware sui dispositivi compromessi. Una volta che il ransomware è stato installato, può bloccare l'accesso ai dati dell'utente o dell'azienda e chiedere un riscatto per ripristinare l'accesso.**
- **In generale, l'utilizzo di exploit CVE è una delle tecniche che gli attaccanti possono utilizzare come opportunità per accedere ai sistemi e migliorare l'efficacia del loro attacco di ransomware.**

Nel primo trimestre 2023 il SOC & Threat Intelligence Team di Swascan ha inoltre individuato le CVE relative al primo trimestre che, vista la severità a loro associate, potrebbero consentire ad un'attaccante di entrare all'interno di infrastrutture ed eseguire codice arbitrario.

Nello specifico tali vulnerabilità potrebbero essere usate con il fine di deployare un Ransomware o infettare massivamente dispositivi con malware (e.g. Information Stealer, RAT).

Di seguito le CVE relative al Q1 2023 rilevate:

CVE ID	Summary	CVSScore
CVE-2023-23397	Microsoft Outlook Elevation of Privilege Vulnerability	9.8
CVE-2023-29059	3CX DesktopApp through 18.12.416 has embedded malicious code, as exploited in the wild in March 2023. This affects versions 18.12.407 and 18.12.416 of the 3CX DesktopApp Electron Windows application shipped in Update 7, and versions 18.11.1213, 18.12.402, 18.12.407, and 18.12.416 of the 3CX DesktopApp Electron macOS application.	N/A
CVE-2023-26359	Adobe ColdFusion versions 2018 Update 15 (and earlier) and 2021 Update 5 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction.	9.8
CVE-2023-21716	Microsoft Word Remote Code Execution Vulnerability	9.8
CVE-2023-21839	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data	7.5
CVE-2023-25610	Vulnerability in FortiOS & FortiProxy. This vulnerability is a buffer underwrite bug in the administrative interface which could allow a remote unauthenticated attacker to execute code using specially crafted requests.	9.3
CVE-2023-23392	Microsoft HTTP Protocol Stack Remote Code Execution Vulnerability	9.8

CVE-2023-27532	Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.	7.5
CVE-2023-20858	VMware Carbon Black App Control 8.7.x prior to 8.7.8, 8.8.x prior to 8.8.6, and 8.9.x.prior to 8.9.4 contain an injection vulnerability. A malicious actor with privileged access to the App Control administration console may be able to use specially crafted input allowing access to the underlying server operating system.	7.2
CVE-2023-25616	In some scenario, SAP Business Objects Business Intelligence Platform (CMC) - versions 420, 430, Program Object execution can lead to code injection vulnerability which could allow an attacker to gain access to resources that are allowed by extra privileges. Successful attack could highly impact the confidentiality, Integrity, and Availability of the system.	8.8

La vulnerabilità CVE-2023-29059 ad esempio, ha consentito al Threat Actor di eseguire un attacco Supply Chain infettando migliaia di dispositivi che utilizzavano l'applicativo. A seguito dell'attacco sono state difatti rilevate numerose Command&Control collegate con l'eseguibile infetto. In questa fase l'attaccante ha quindi potenzialmente avuto accesso a un numero molto elevato di asset aziendali compromettendo quindi la confidenzialità del dato di molte compagnie.

Oltre alle CVE in questione è da notare che le vulnerabilità critiche identificate hanno un impatto più devastante tenendo conto che fanno riferimento a sistemi estremamente diffusi e utilizzati

Questo solleva e riconferma sempre di più non solo il problema della Supply chain, ma non solo. Uno spazio temporale tra la segnalazione della vulnerabilità, il rilascio della relativa patch e il tempo necessario per i Dipartimenti IT di aggiornare i sistemi. Questo tempo rappresenta l'opportunità degli attaccanti. Tempo che diventa sempre più ampio soprattutto in contesti in cui diversi sistemi sono tra loro interconnessi. Poiché l'aggiornamento di un sistema non garantisce che tutto il resto continui a funzionare.

LA MINACCIA RANSOMWARE

898 obiettivi attaccati in 79 paesi diversi nel primo trimestre del 2023, con una crescita del 19% rispetto al 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 Q1 2023.

In particolare, sono stati raccolti, attraverso specifiche ricerche OSINT & CLOSINT, i dati che riguardano le vittime delle 15 gang Ransomware più attive nel primo trimestre del 2023:

LockBit	CLOP	Alphav/BlackCat	Royal	BlackBasta
PLAY	Vice Society	Medusa	BianLian	Stormous
AvosLocker	RansomHouse	Mallox	BlackByte	DarkPower

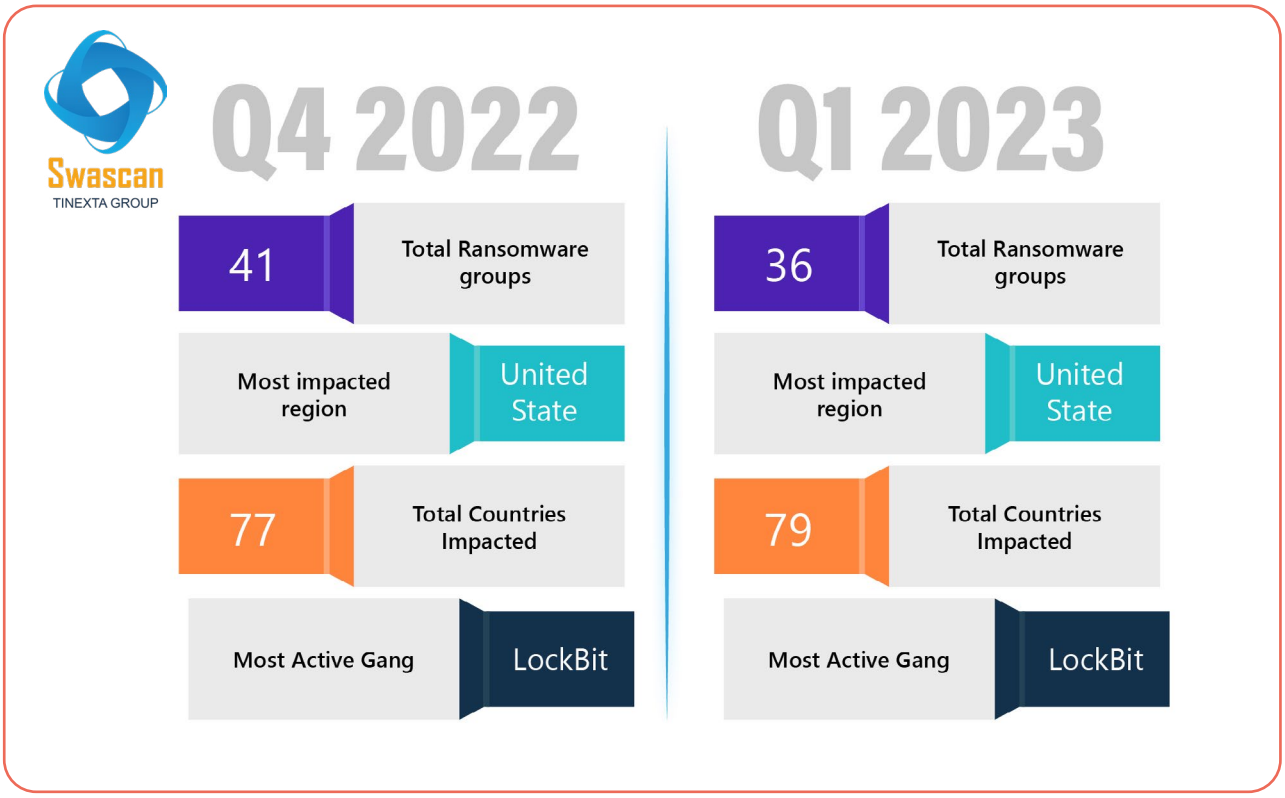
L'approccio metodologico utilizzato è stato il seguente:

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**

Il contesto

A livello globale, è possibile osservare un incremento nel numero delle vittime rispetto al Q4 2022 e un lieve incremento dei paesi colpiti, ma un decremento del 12% rispetto del numero delle gang attive, per un totale di 36 nell'ultimo trimestre:



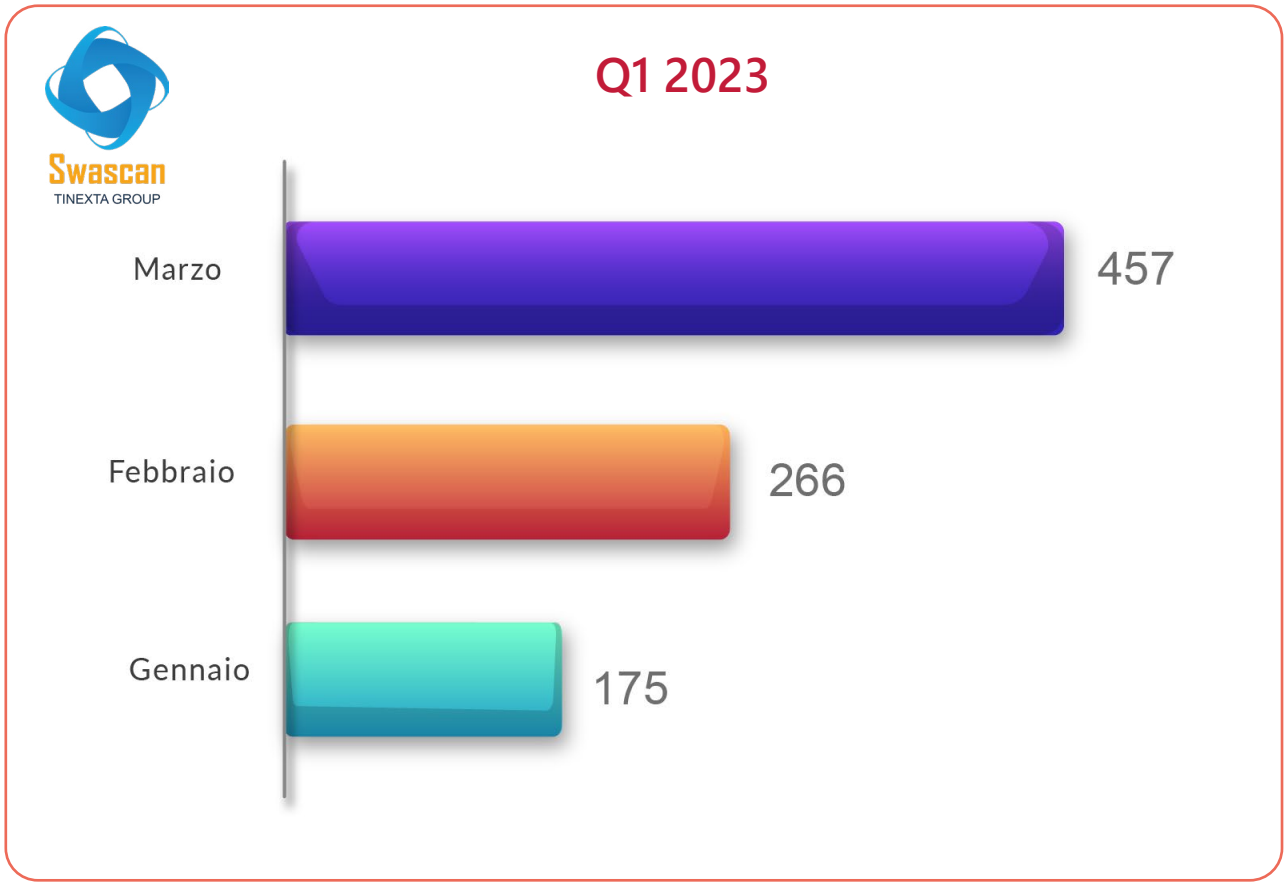
Focalizzandoci sul Q1 2023, si riscontrano:

1. **+161% di vittime** dall'inizio dell'anno: nel dettaglio, la percentuale di rialzo tra gennaio e febbraio è del 52%, mentre quella tra febbraio e marzo è del 72%.

2. **Aumento** delle vittime rispetto al Q4 2022 del 19%.

3. **Aumento** di vittime in Italia rispetto al Q4 2022 dove il totale delle aziende colpite era di 14, mentre nell'ultimo trimestre salgono a 26.

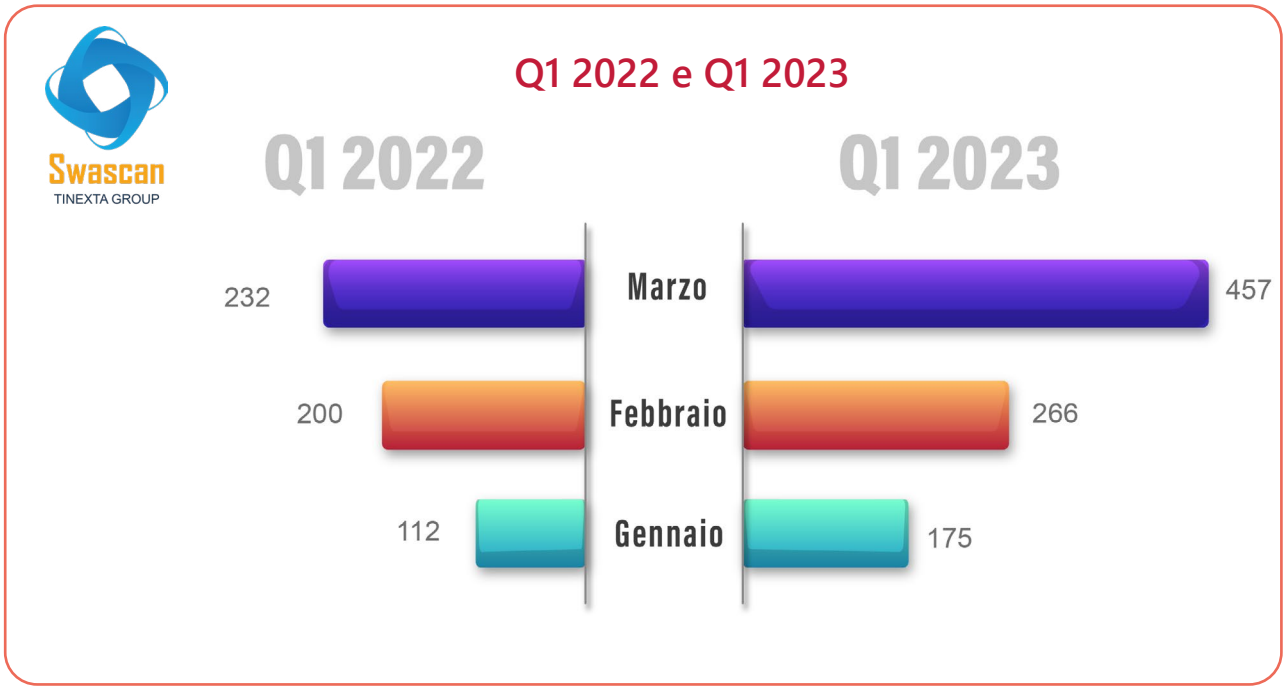
Durante il trimestre considerato, si è registrato un aumento costante del numero di attacchi. In particolare, il numero è salito da 175 nel mese di gennaio a 266 in febbraio e infine a 457 nel mese di marzo, indicando una tendenza al rialzo. Questa crescita potrebbe essere causata da diversi fattori, come l'aumento della sofisticazione delle tecniche di attacco, la diffusione di vulnerabilità o la mancanza di misure di sicurezza adeguate da parte delle organizzazioni target. Tuttavia, è importante notare che i numeri forniti rappresentano solo una parte dei potenziali attacchi, in quanto molti di essi potrebbero non essere stati rilevati o segnalati.



Inoltre, comparando il Q1 2022 e il Q1 2023 riscontriamo un aumento di attacchi del 21%.

In particolare, nel **gennaio 2023** si sono verificati **175 attacchi ransomware**, rispetto ai 112 attacchi registrati nello stesso periodo dell'anno precedente. Questo rappresenta un **aumento del 56%,** che suggerisce come gli attacchi ransomware stiano diventando sempre più comuni.

Il numero di attacchi ransomware è aumentato ancor di più a febbraio e marzo 2023, passando rispettivamente a 266 e 457 attacchi, contro i 200 e 232 dello stesso periodo dello scorso anno.



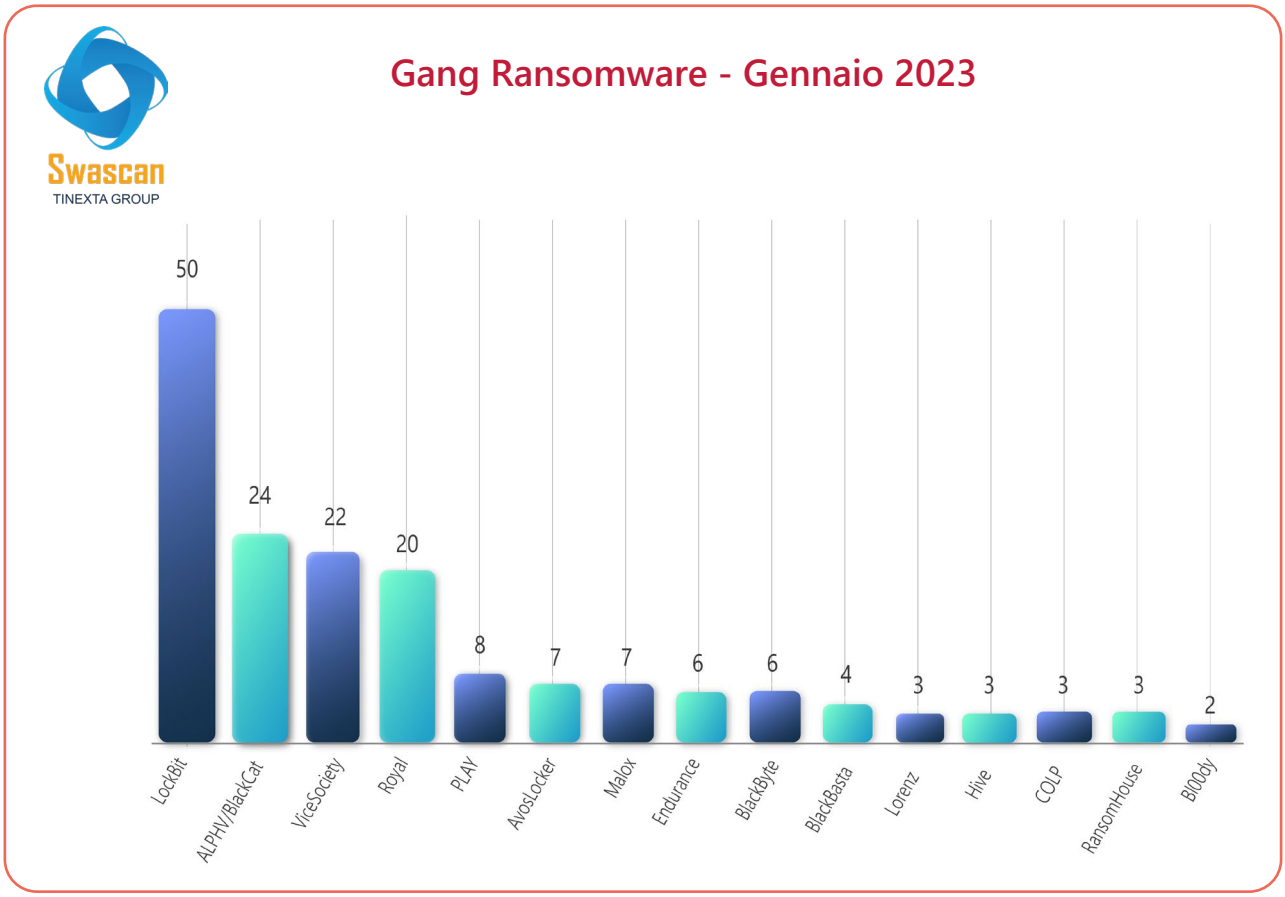
Le Gang più attive nel Q1 023

La gang **LockBit** ha condotto ben **277 attacchi**, mantenendo il primato tra le gang più attive e pericolose. **CLOP**, che ha preso di mira numerose organizzazioni governative e aziendali, ha effettuato **106 attacchi**, mentre **ALPHV/BlackCat** ha raggiunto un totale di **94 attacchi**.

Altre gang che si sono distinte per il loro alto livello di attività sono Royal, che ha effettuato 66 attacchi, PLAY, con 41 attacchi, e ViceSociety, con 32 attacchi.

Di seguito la classifica delle gang ransomware più attive:

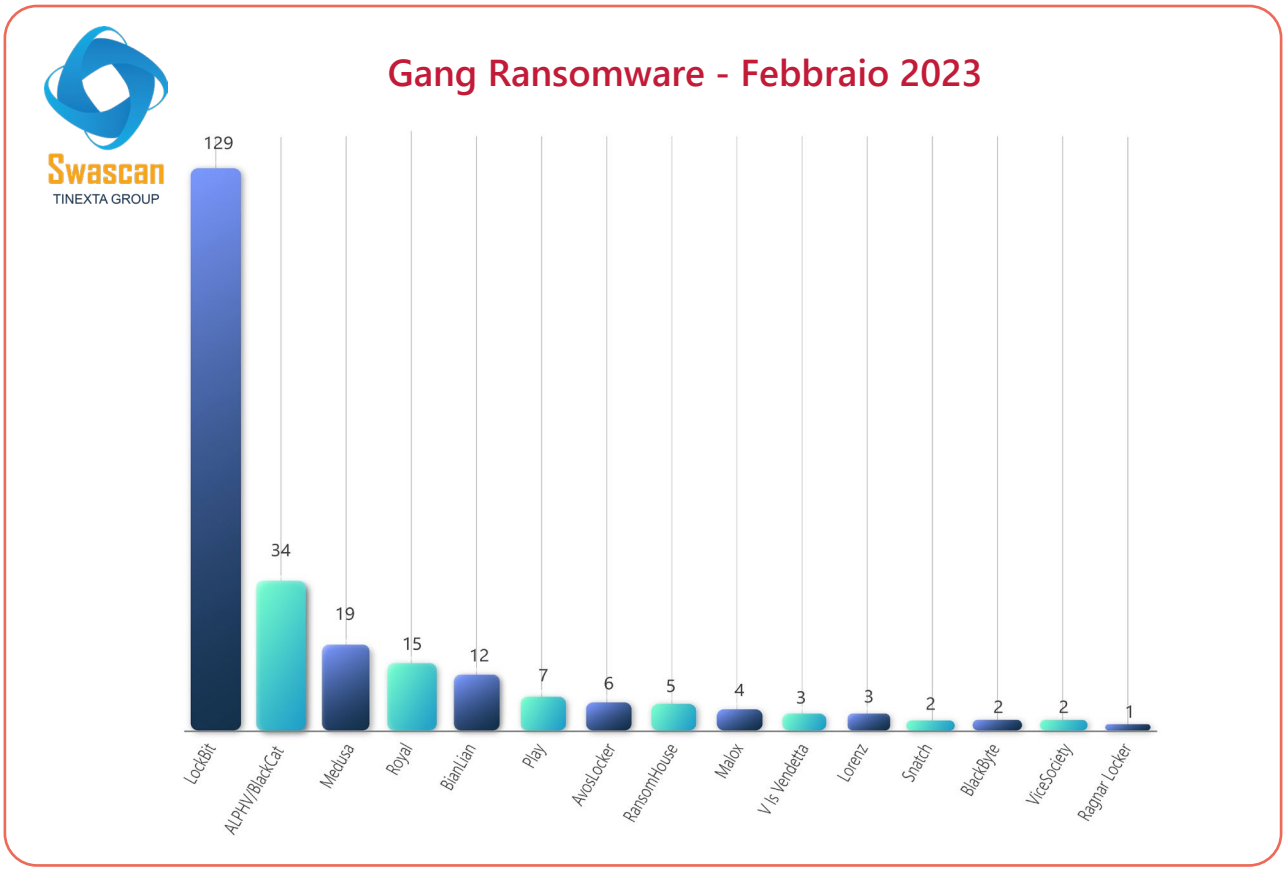
A seguire viene mostrata l'analisi relativa ad ogni singolo mese del Q1 2023. Per il solo mese di Gennaio 2023, queste le gang ransomware più attive:



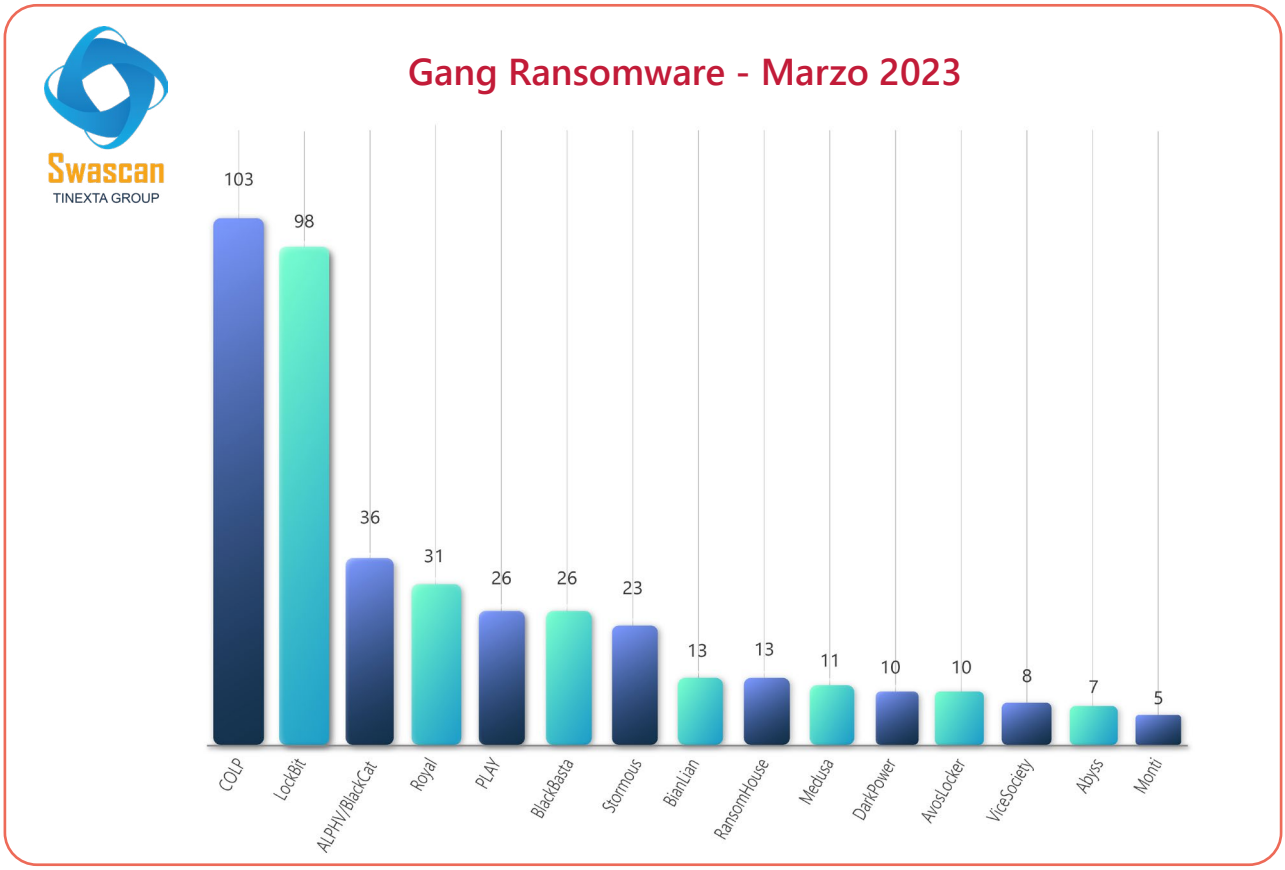
A gennaio, Vice Society ha reso pubblici i dati di nove scuole sul suo sito di leak: si tratta della gang che più si concentra sui distretti scolastici come bersagli, motivo per cui il settore dell'istruzione è stato vittima di attacchi informatici sempre più frequenti nell'ultimo trimestre.

L'attività del gruppo Play ha subito una forte diminuzione rispetto a dicembre, mentre AvosLocker, un gruppo precedentemente inattivo dal mese di ottobre 2022, è tornato alla ribalta.

Nel mese di Febbraio 2023 risale in modo esponenziale il numero degli attacchi della gang LockBit, con un totale di 129 vittime. Non si è avuto invece alcun segnale da un altro noto player, la gang BlackBasta. Dalla sua apparizione nell'aprile del 2022, è stata una costante vederlo tra i primi posti della classifica dei gruppi di ransomware. Tuttavia, la presunta inattività dei gruppi di ransomware è complicata dal fatto che sui loro siti nel Dark Web riportano solo le aziende che non hanno pagato il riscatto. Ciò significa che un mese estremamente redditizio per questi gruppi può apparire come un mese in cui non sono attivi. Inoltre, il sito Tor di Black Basta News, dove vengono pubblicate le nuove vittime, è stato offline per diverse settimane.



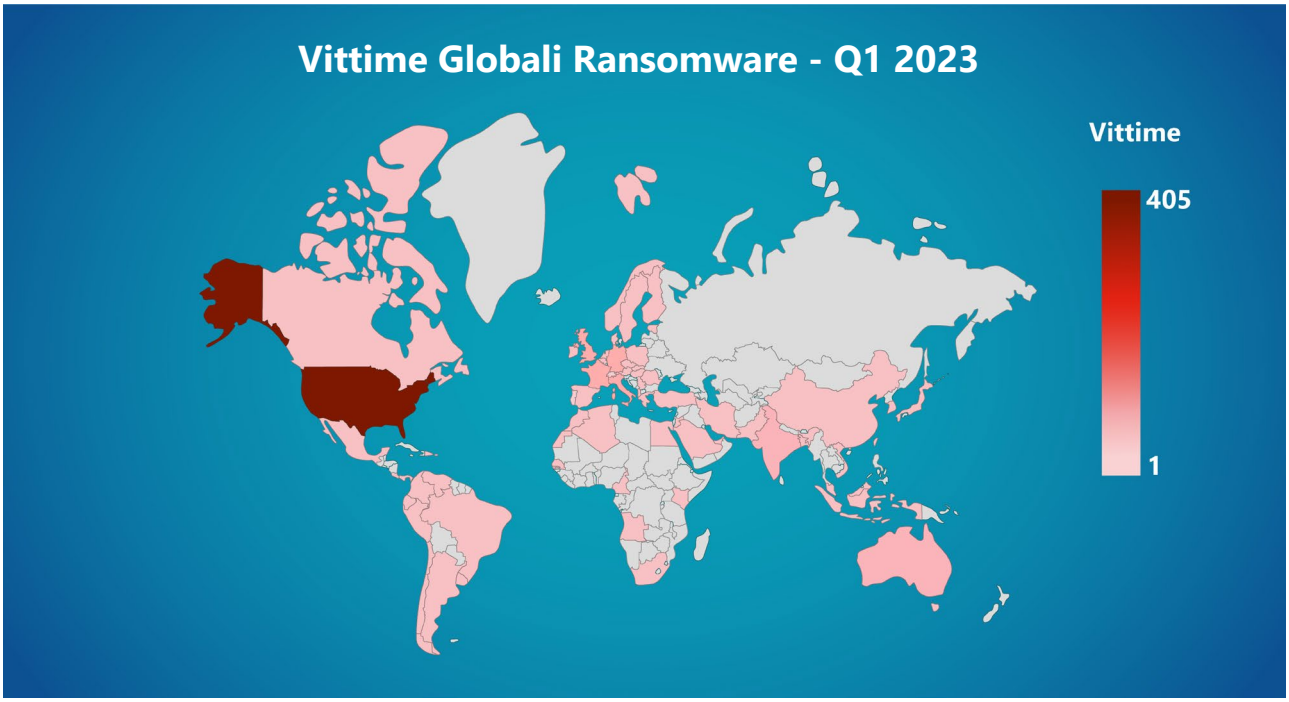
Per il mese di marzo 2023, la gang Clop passa in testa alla classifica con un totale di 103 attacchi contro i 98 di LockBit:



Distribuzione geografica globale delle vittime

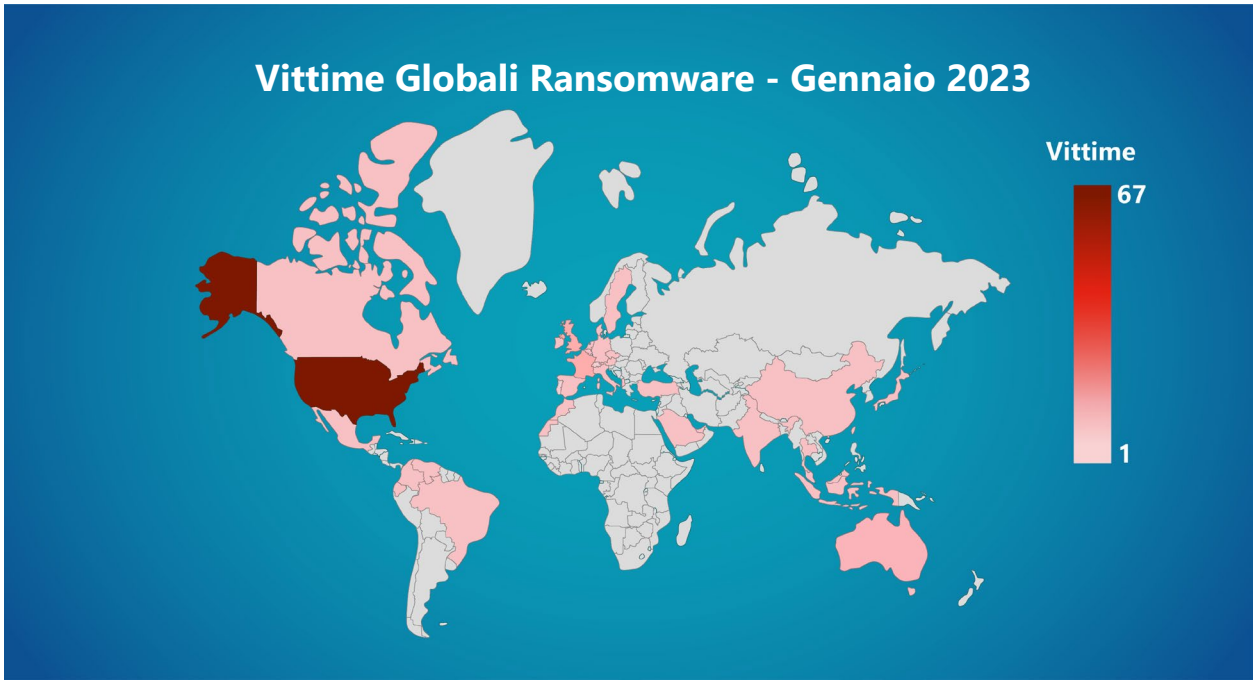
Gli Stati Uniti si confermano al primo posto con un totale di 275 attacchi nel corso dell'ultimo trimestre del 2022, mentre l'Italia scende al 10° posto (rispetto al sesto del mese precedente). Tra i paesi europei passa al primo posto la Germania con un totale di 29 vittime.

Nelle mappe di seguito, la distribuzione geografica degli attacchi ransomware nel primo trimestre 2023.



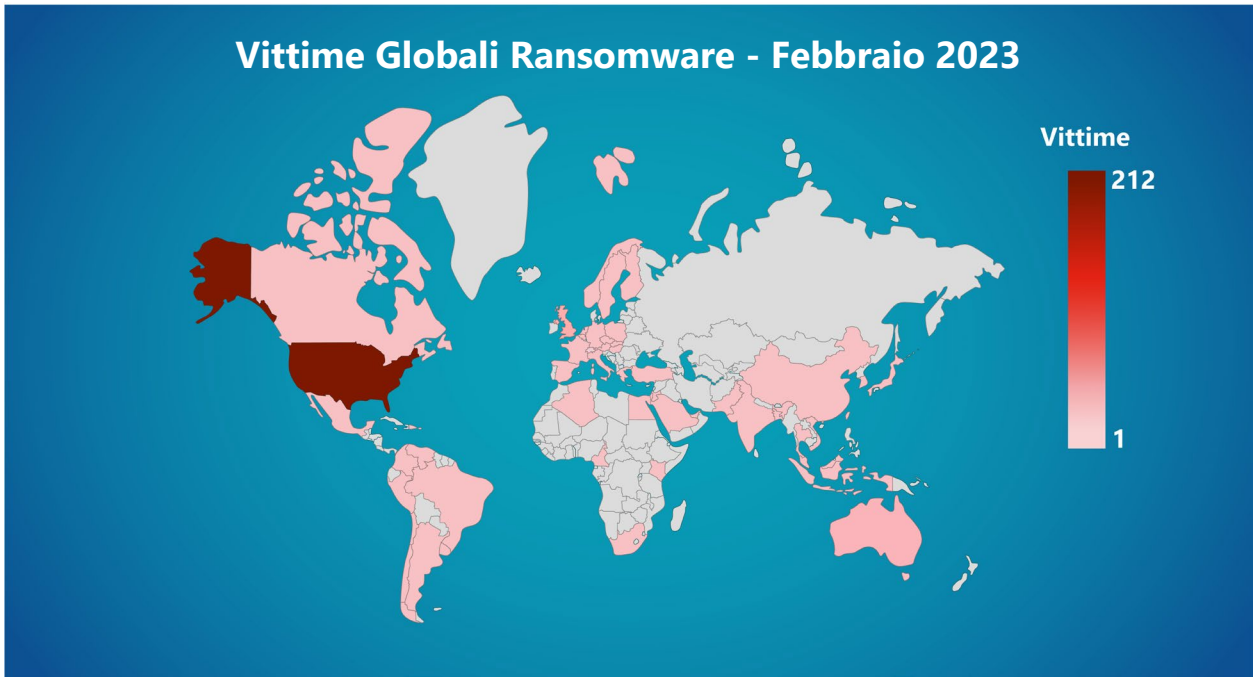
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – Q1 2023
United States	405
United Kingdom	63
Canada	47
France	34
Germany	28
Italy	26
India	24
Australia	19

Nel mese di gennaio si contano un totale di 37 paesi attaccati, con 67 vittime negli Stati Uniti. Nello stesso mese, in Italia il numero di aziende colpite è 5.



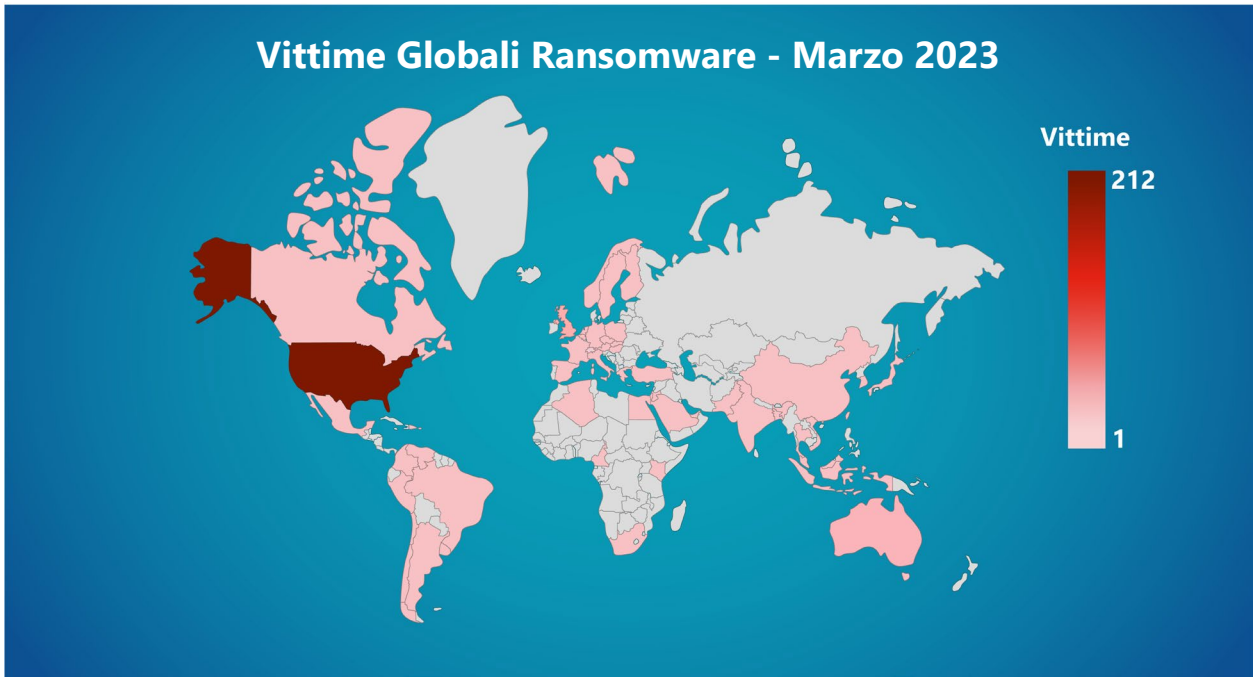
PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – gennaio 2023
United States	67
United Kingdom	18
Australia	7
Canada	7
France	7
Italy	5
Mexico	5
Belgium	4

Stesso discorso per il mese di febbraio, in cui gli Stati Uniti contano un totale di 126 vittime. Salgono anche le vittime in Italia, per un totale di 9 nel mese preso in analisi.



PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – febbraio 2023
United States	126
United Kingdom	16
Canada	10
France	10
Germany	9
Italy	9
Brazil	6
Australia	5

Anche a marzo 2023 il più alto numero di vittime è riscontrato negli Stati Uniti (212). Nello stesso mese, in Italia se ne contano 12.



PAESE	Numero di aziende vittime di Ransomware con dati pubblicati – marzo 2023
United States	212
Canada	30
United Kingdom	29
France	17
Germany	16
India	15
Italy	12
Spain	12

I settori presi di mira dalla minaccia ransomware

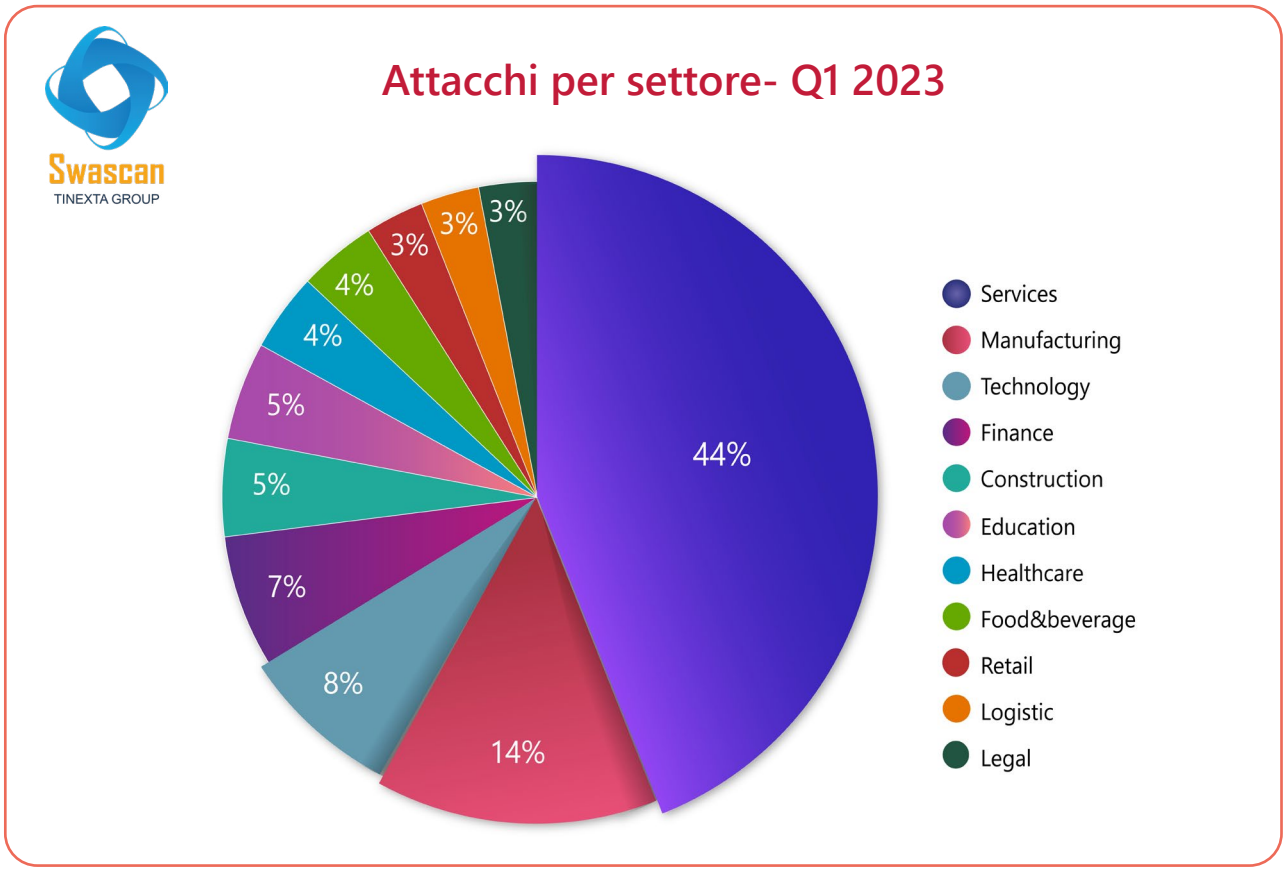
Negli ultimi mesi, il ransomware ha continuato a rappresentare una grave minaccia per le organizzazioni di diversi settori, causando danni finanziari significativi e mettendo a rischio la sicurezza dei dati sensibili.

Secondo gli ultimi dati, nel primo trimestre del 2023 il settore più colpito è stato quello dei servizi: questi attacchi hanno colpito un'ampia gamma di organizzazioni, dalle piccole imprese alle grandi multinazionali, causando interruzioni nei servizi e danni finanziari considerevoli. In seconda posizione si trova il settore manifatturiero, spesso bersaglio a causa della sua dipendenza dai sistemi tecnologici per il controllo dei processi di produzione, il che lo rende particolarmente vulnerabile.

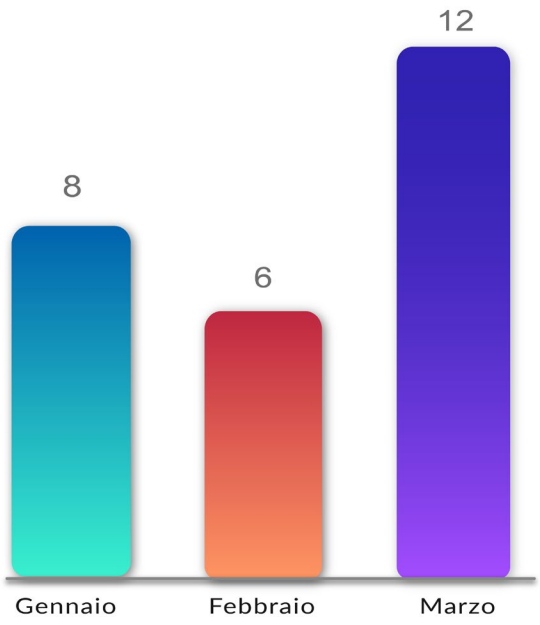
Al terzo posto si trovano il settore tecnologico e quello finanziario: anche in questi casi, le organizzazioni di questi settori gestiscono grandi quantità di dati sensibili e finanziari, il che li rende obiettivi appetibili per le gang ransomware.

In generale, i dati dimostrano che nessun settore è escluso dalla minaccia dei ransomware e che tutte le organizzazioni, indipendentemente dal settore in cui operano, devono adottare misure adeguate per proteggere i propri sistemi e i propri dati.

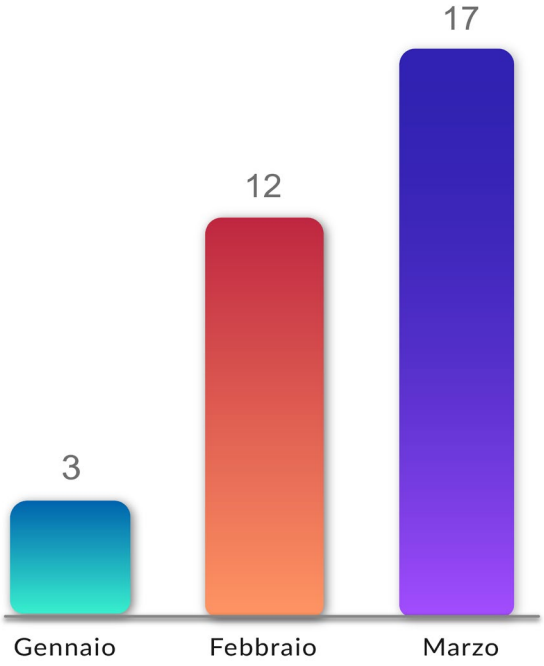
Di seguito un'analisi dei settori e delle infrastrutture critiche colpite nel Q1 2023:



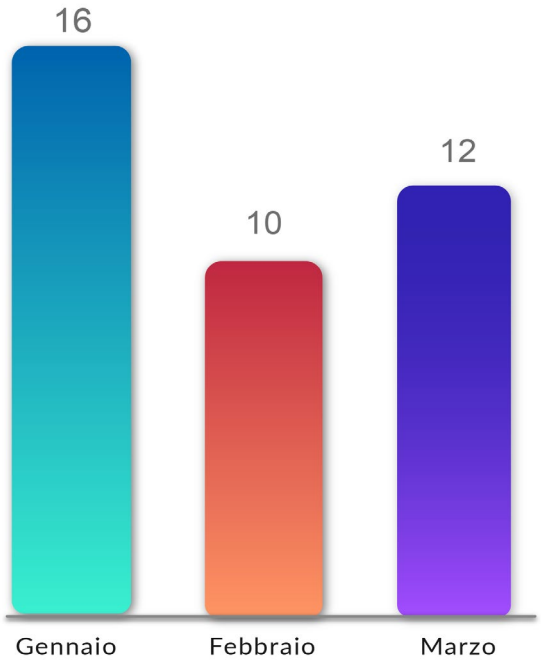
Attacchi Ransomware a Strutture Sanitarie



Attacchi Ransomware ad Amministrazioni Statali e Comunali



Attacchi Ransomware a Distretti Scolastici e Universitari



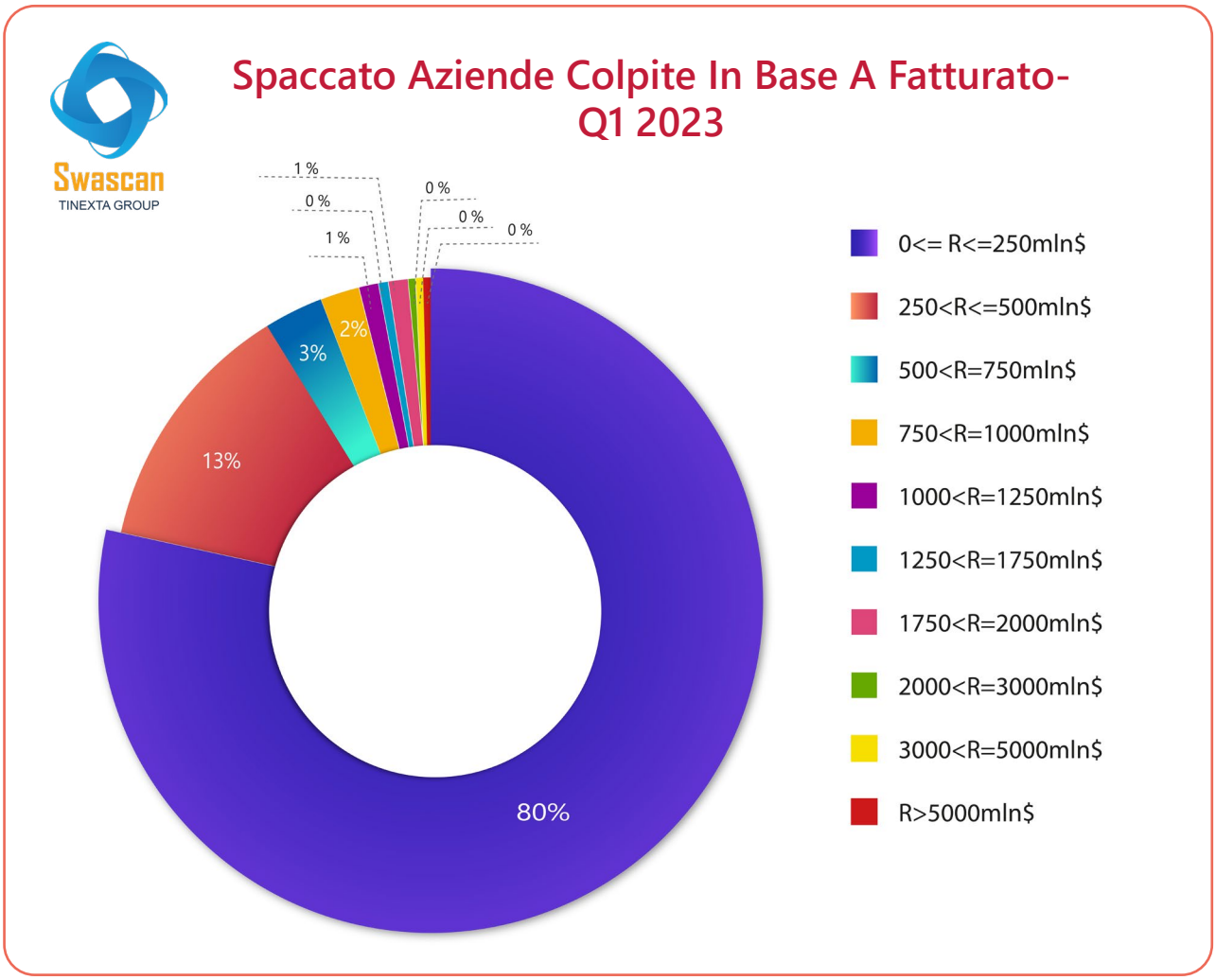
I Settori più colpiti

Cluster vittime in base a personale e fatturato

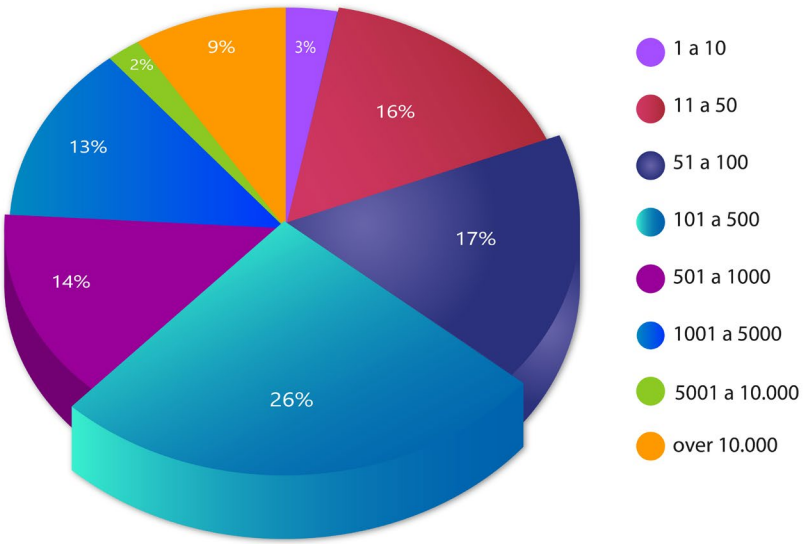
Le statistiche confermano l'attenzione verso le PMI a causa della loro vulnerabilità alle minacce informatiche. Le PMI spesso hanno meno risorse finanziarie e tecniche rispetto alle grandi imprese per investire in sicurezza informatica, e possono diventare bersaglio facile per gli attacchi informatici.

Le aziende colpite in base al fatturato

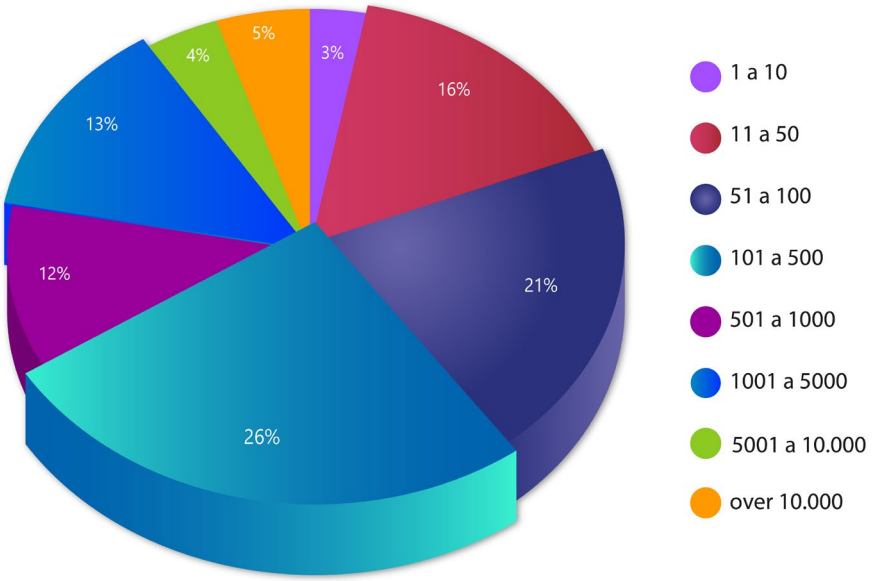
I dati mostrano chiaramente che gli attacchi ransomware si concentrano principalmente sulle piccole e medie imprese (PMI) con un fatturato annuo inferiore a 250 milioni di dollari: l'80% degli attacchi ha infatti come obiettivo le aziende che rientrano in questa fascia di fatturato.

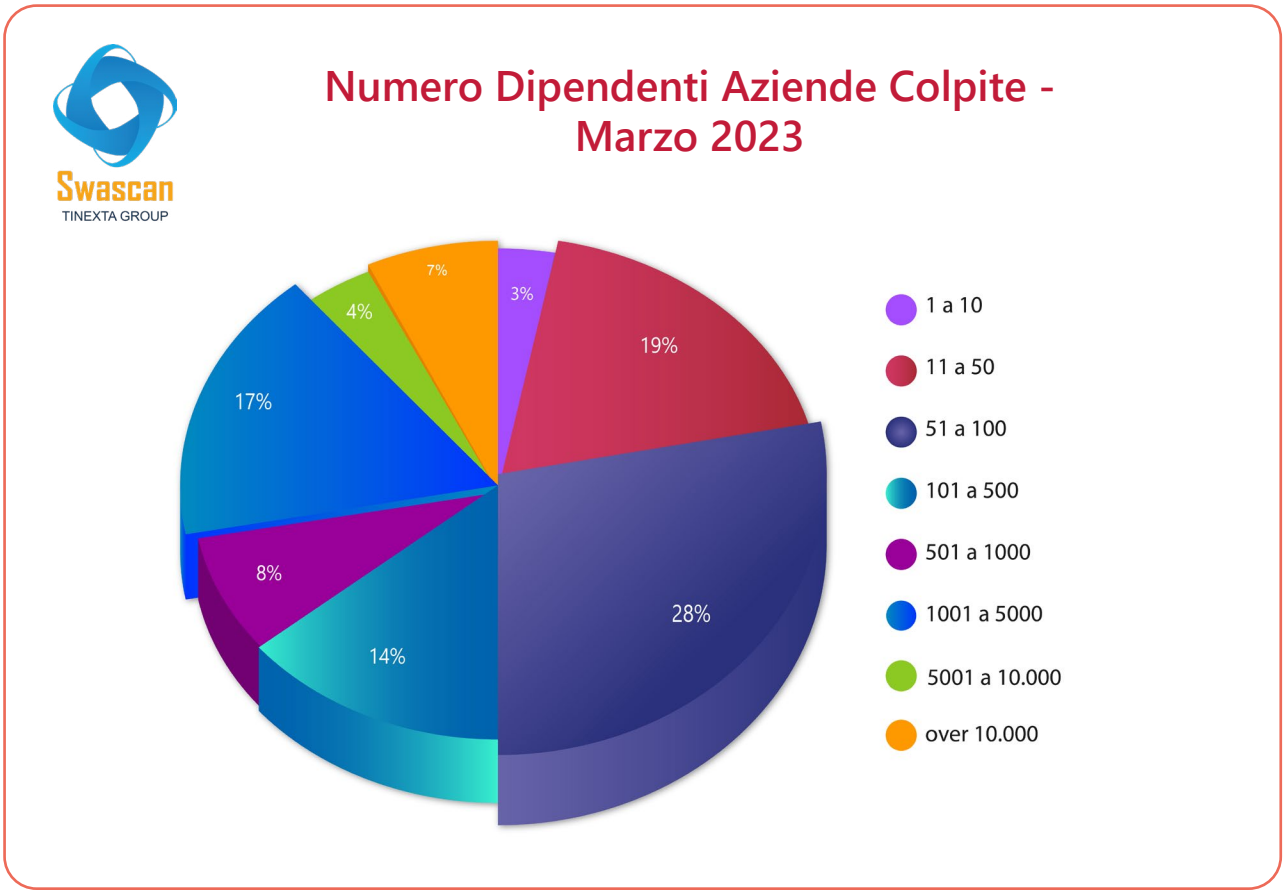


Numero Dipendenti Aziende Colpite - Gennaio 2023



Numero Dipendenti Aziende Colpite - Febbraio 2023




Swascan
TINEXTA GROUP
Numero Dipendenti Aziende Colpite - Marzo 2023
3%
19%
28%
14%
8%
17%
4%
7%
1 a 10
11 a 50
51 a 100
101 a 500
501 a 1000
1001 a 5000
5001 a 10.000
over 10.000

CONCLUSIONI

Il primo trimestre del 2023 ha visto la minaccia del ransomware continuare a seminare il caos nelle organizzazioni di tutto il mondo. Secondo i dati recenti, sono state identificate 36 diverse gruppi di ransomware operanti, con gli Stati Uniti che sono risultati essere la regione più colpita e un totale di 79 paesi che hanno subito attacchi. Tra i gruppi più attivi, spicca LockBit, che ha causato notevoli danni a molte organizzazioni, raggiungendo un totale di 277 attacchi.

Il quadro generale del Q1 2023 indica un preoccupante aumento del numero di vittime del ransomware rispetto ai trimestri precedenti. Le percentuali di crescita registrate sono state particolarmente significative, con un aumento del 104% confrontando i mesi di gennaio e marzo e un aumento del 19% rispetto al Q4 2022. Concentrando l'attenzione sui dati emerge che gli Stati Uniti hanno subito il maggior numero di attacchi con 405 aziende vittime. Seguono il Regno Unito con 63 aziende colpite e il Canada con 47. Tuttavia, è allarmante notare che anche l'Italia si posiziona tra i primi paesi a livello di numero di aziende colpite, con un totale di 26. Questo rappresenta un significativo aumento rispetto al trimestre precedente, e indica la necessità urgente di adottare misure di sicurezza adeguate a proteggere le aziende italiane dalle minacce del ransomware. Si rende, quindi, necessario un maggiore investimento in soluzioni tecnologiche avanzate per prevenire e contrastare gli attacchi ransomware e per garantire la sicurezza dei dati e delle attività delle organizzazioni italiane.

Inoltre, nel trimestre considerato, il numero di attacchi ransomware registrati nel paese è aumentato del 56% rispetto allo stesso periodo dell'anno precedente, passando da 112 a 175. Tuttavia, il dato più allarmante è la crescita esponenziale degli attacchi nei mesi successivi. Nel mese di febbraio, gli attacchi sono saliti a 266, mentre nel mese di marzo il numero ha raggiunto i 457, un aumento significativo rispetto ai 200 e 232 attacchi rispettivamente registrati nei mesi corrispondenti dell'anno precedente. Inoltre, la quantità di attacchi ransomware nel Q1 2023 è aumentata del 21% rispetto al Q1 2022, passando da 741 a 898.

LockBit è risultata essere la più attiva, seguita da CLOP con 106 attacchi e da Alphav/BlackCat con 94 attacchi. Si tratta di un mondo in costante evoluzione, con alcuni gruppi in rapida ascesa e altri che subiscono un calo. Questo è il caso di Vice Society, che ha visto una crescita del 267% nella sua attività di attacco continuato a concentrarsi sui settori sensibili e in particolare sull'istruzione, mentre AlphV ha invece subito un calo del 25% degli annunci da dicembre a gennaio. Marzo il mese con il più alto numero di vittime, in cui la gang ransomware CLOP sorpassa LockBit.

Rimane sempre alta l'attenzione alle PMI, considerate i soggetti più deboli.

I dati mostrano chiaramente che gli attacchi ransomware si concentrano principalmente sulle piccole e medie imprese: **l'80% degli attacchi** ha infatti come obiettivo **le aziende con un fatturato inferiore ai 250 milioni di euro,** mentre il **62% degli attacchi** ha riguardato realtà con **meno di 500 dipendenti.**

La minaccia del malware continua a rappresentare una preoccupazione per le aziende e i consumatori in tutto il mondo. Secondo gli ultimi dati, i malware più diffusi sono il Mirai e l'Hajime, con il 33% e il 34% rispettivamente. Seguono poi RecordBreaker con il 12%, Gozi con l'11% e Emotet con il 10%. La crescita della popolarità e dell'accessibilità degli stealer e di altri tipi di malware rappresenta una preoccupazione sempre più grande per le aziende e gli individui che cercano di proteggere i propri dati e le proprie informazioni sensibili. Come riportato dai dati più recenti, la facilità di accesso a questi strumenti ha spinto molti Threat actors, di ogni livello di abilità, a cercare mercati illeciti dove vendere il crimeware. La maggior parte di questi servizi, infatti, è stata pubblicizzata e discussa sui forum open-source, come XSS, Exploit e BreachForum.

Inoltre, la sofisticazione di questi malware è in costante evoluzione, il che rende sempre più difficile la loro identificazione e rimozione. La tendenza del 2023 è quella di una continua crescita dell'uso degli stealer e di altri tipi di malware, il che rende ancora più importante la necessità di adottare misure di sicurezza adeguate a prevenire e gestire gli attacchi informatici.

A fronte di questo scenario in continua evoluzione, le aziende e gli individui devono rimanere vigili e adottare misure proattive per proteggere i propri dati e le proprie informazioni sensibili. Ciò include l'utilizzo di strumenti di sicurezza affidabili, l'adozione di politiche di sicurezza informatica efficaci e la formazione del personale su come identificare e gestire le minacce informatiche. Solo attraverso un'azione tempestiva e una costante attenzione alla sicurezza informatica, sarà possibile proteggere sé stessi e i propri dati dai sempre più sofisticati attacchi informatici degli stealer e di altri tipi di malware.

Il phishing, infine, continua ad essere tra i primi vettori di attacco: Facebook, con il 18% degli attacchi, è la piattaforma più utilizzata per condurre attacchi, seguita da Office365 e Bet365. Nonostante i miglioramenti in termini di sicurezza informatica, è importante che le aziende adottino misure di sicurezza efficaci per proteggere i propri utenti e sensibilizzarli sui pericoli del phishing. Il fatto che uno strumento progettato per gli ambienti tipicamente lavorativi, come la suite di Office, venga utilizzata come esca dagli aggressori è una prova schiacciante di come le tecniche di BEC la facciano ancora da padrone.

Previsioni Q2 2023

1. Il ransomware rimarrà il prodotto più utilizzato dai Criminal Hacker.
2. Nuove gang ransomware si stanno facendo strada per numero di vittime colpite dimostrando una particolare attenzione nelle campagne di affiliazione.
3. Nel mondo malware dovremo affrontare un incremento del mondo degli Infostealer che adotteranno maggiori funzionalità, saranno adattabili al contesto e sempre di più strumento di driver per gli attacchi ransomware.
4. Il phishing rimarrà l'evergreen con un incremento del mondo smishing.
5. Incremento di vulnerabilità critiche relative a prodotti software diffusi e di uso comune.
6. Cyber war e mondo antagonista avranno un loro ruolo nel contesto dei rischi informatici in azioni di cyberspionaggio e sabotaggio.
7. Incremento delle operazioni di polizia al contrasto del mondo criminale soprattutto a livello i darkweb.

Punti di Attenzione

1. L'incremento e attenzione per il mondo dati/informazioni/credenziali impone la necessità di una attività di sensibilizzazione che deve essere rivolta in primis ai cittadini attraverso azioni a livello di governo.
2. La PMI rimane il target di riferimento, questo rende fortemente consigliato un incentivo agli investimenti di cyber security puntando a sistemi di defiscalizzazione sugli investimenti in cyber.
3. È anche auspicabile garantire un accesso agevolato al mondo del PNRR a questo settore critico della nostra economia.

Il commento del CEO di Swascan, Pierguido Iezzi

"L'attenzione dei Criminal Hacker nei confronti del mondo delle credenziali, fortunatamente non è passata in sordina. Negli ultimi mesi le autorità internazionali hanno infatti chiuso due dei principali market per la compravendita di informazioni rubate. Questo però ha portato i criminali informatici a ripiegare in maniera più massiccia sul mondo dei trojan e infostealer per avere queste informazioni, adesso non più così facilmente reperibili", spiega il CEO di Swascan Pierguido Iezzi.

"Quanto riportato in questo studio ci da un'idea degli scenari futuri di evoluzione del mondo del cyber crime. Per contrastare la continua crescita di questo mondo è necessario quindi giocare d'anticipo, in particolare andando ad anticipare i vettori d'attacco e agendo in maniera preventiva e proattiva sui singoli steps della cyber kill chain prima che vengano conclusi nella loro interezza".

"Questo passa non solo per le misure tecniche di sicurezza predittiva, preventiva e proattiva, ma anche attraverso una generale e diffusa opera di sensibilizzazione nei confronti delle minacce. Sia nel mondo del privato sia nel mondo del pubblico".

"È anche auspicabile che, per quanto riguarda il nostro sistema-Paese, non si fermino le opere in supporto alla difesa cyber delle aziende. Quanto di buono è stato fatto – e verrà fatto – tramite il PNRR, potrebbe essere affiancato da un'ulteriore defiscalizzazione degli investimenti nel campo della cyber security".

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**

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

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** è parte integrante del Gruppo **Tinexta S.P.A.** azienda quotata sul segmento STAR di Borsa Italiana

Swascan è diventata 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 identità digitale e sicurezza digitale.

Analysis by:

Martina Fonzo
Fabio Pensa

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