



**Swascan**  
TINEXTA GROUP



# Threatland Q2

Trend e scenari del  
Cybercrime

[www.swascan.com](http://www.swascan.com)  
[info@swascan.com](mailto:info@swascan.com)

# Sommario

Cyber risk summary .....	Pg. 03
La cyber kill chain: un approccio strategico per difendersi dagli attacchi informatici .....	Pg. 05
Reconnaissance .....	Pg. 07
Compromised devices, credential leaks & social engineering .....	Pg. 08
Social engineering .....	Pg. 12
Common Vulnerabilities and Exposures .....	Pg. 14
Weaponization .....	Pg. 17
Malware .....	Pg. 18
Delivery .....	Pg. 19
Phishing .....	Pg. 20
Exploitation .....	Pg. 24
CVE .....	Pg. 25
Command&Control .....	Pg. 28
Actions on Objectives .....	Pg. 30
Attacchi ransomware .....	Pg. 32
Le gang ransomware più prolifiche .....	Pg. 36
Distribuzione geografica globale delle vittime .....	Pg. 37
I settori presi di mira dalla minaccia ransomware .....	Pg. 42
Cluster vittime in base a personale .....	Pg. 43
Focus Italia .....	Pg. 45
Conclusioni .....	Pg. 50
Come difendersi dal Ransomware: Il Cyber Security Framework .....	Pg. 54
Action Plan .....	Pg. 55
Disclaimer .....	Pg. 58
About us .....	Pg. 59



## CYBER RISK SUMMARY

---

- **1451 vittime** di attacchi ransomware nel Q2 2023, **un aumento del 62%** rispetto al trimestre precedente.
- **Le PMI**, in particolare le piccole micro-aziende, si sono confermate **il target preferito dai Criminal Hacker. (80%)**
- A livello globale **le aziende di servizi** sono **le più colpite** dalle gang ransomware. **(47%)**
- **+34.6%** il numero di **attacchi nel nostro paese** rispetto al trimestre precedente.
- **Gli infostealer** si confermano la famiglia di **malware più diffusa**.
- **Microsoft** il brand **più imitato** per le campagne di phishing.

Il secondo trimestre del 2023 ha visto un aumento significativo di attacchi informatici mirati al furto di dati e alla richiesta di riscatto in cambio del ripristino dei sistemi colpiti. Il **SOC e Threat Intelligence Team di Swascan** ha condotto un'analisi approfondita sugli scenari ransomware, malware e phishing, fornendo un quadro dettagliato delle minacce emergenti e delle tendenze in evoluzione.

Durante il Q2 sono state osservate numerose campagne ransomware, caratterizzate dalla diffusione di software malevoli che criptano i dati delle vittime e richiedono poi un riscatto per ripristinarli. Questi attacchi hanno colpito una vasta gamma di settori, inclusi quelli finanziari, sanitari, governativi, mettendo a rischio la sicurezza delle informazioni e la continuità operativa.

L'evoluzione delle tattiche utilizzate dai criminali informatici nel Q2 è stata particolarmente preoccupante. I ransomware sono diventati sempre più sofisticati e mirati e sono emerse numerose nuove gang ransomware.

Parallelamente agli attacchi di ransomware, il phishing ha continuato a rappresentare una minaccia significativa per la sicurezza informatica nel Q2. Gli attaccanti hanno utilizzato metodi sempre più sofisticati per ingannare gli utenti, creando e-mail, siti web e messaggi di testo ingannevoli che sembrano provenire da fonti legittime. Attraverso queste tecniche, gli attaccanti cercano di ottenere informazioni sensibili come password, dati finanziari e credenziali di accesso, al fine di compiere frodi e danneggiare le vittime.

In questo report, analizzeremo i principali attacchi ransomware e phishing registrati nel Q2 2023, evidenziando le modalità operative, le vittime, le regioni colpite e le tendenze emergenti, ed esamineremo le misure di sicurezza consigliate per mitigare il rischio di tali minacce.

Il secondo 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.

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: un approccio strategico per difendersi dagli attacchi informatici

*La Cyber Kill Chain è un modello utilizzato in sicurezza informatica per descrivere le fasi tipiche di un attacco informatico, in modo da comprendere meglio come gli attaccanti possono penetrare nei sistemi e danneggiarli.*

Nel panorama sempre più complesso e frequente degli attacchi informatici, la Cyber Kill Chain si presenta come uno strumento fondamentale per identificare e contrastare le minacce provenienti dai criminal hacker. Questa metodologia di difesa, ispirata al concetto di Kill Chain utilizzato in campo militare, è stata adottata nel settore della cyber security al fine di individuare le fasi attraverso le quali un attacco si sviluppa e di preparare una strategia difensiva adeguata e si compone di sette fasi ben definite. Queste fasi rappresentano i passaggi che un potenziale criminal hacker dovrebbe compiere per portare a termine un attacco e consentono di comprendere il modus operandi degli aggressori, individuando i segnali di attacco e mettendo in atto le necessarie contromisure.



Le sette fasi della Cyber Kill Chain sono le seguenti:

- 1. Reconnaissance:** in questa fase il criminal hacker individua il bersaglio e conduce una ricerca approfondita per identificare le vulnerabilità presenti nel sistema di sicurezza del target. Questa fase è di fondamentale importanza poiché determina il successo delle fasi successive.
- 2. Weaponization:** nel secondo step l'attaccante utilizza le informazioni raccolte nella fase precedente per selezionare gli strumenti più adatti a creare un accesso remoto al sistema bersaglio.
- 3. Delivery:** in questa fase, il malware creato viene consegnato al bersaglio attraverso diversi vettori, come ad esempio mail di phishing o link presenti su siti web compromessi.
- 4. Exploitation:** una volta consegnato al bersaglio, il malware viene attivato e sfrutta le vulnerabilità del sistema per ottenere un accesso non autorizzato o eseguire altre azioni malevole.
- 5. Installation:** durante la fase di installation, l'attaccante si assicura di installare ed eseguire il malware nel sistema bersaglio. Questo gli consente di aggirare i controlli di sicurezza e mantenere l'accesso al sistema. L'installazione del malware avviene grazie all'exploit selezionato durante la fase di weaponization e viene eseguita durante la fase di exploitation.
- 6. Command & Control:** nel sesto step della catena, gli attaccanti stabiliscono una connessione tra il sistema vittima e la macchina remota da cui operano. Questa connessione permette loro di ottenere un controllo persistente e un accesso continuo all'ambiente della vittima.
- 7. Actions on Objectives:** nell'ultimo anello della catena, gli attaccanti portano a termine l'attacco colpendo l'obiettivo prefissato, e questo può portare alla manipolazione dei dati, l'esfiltrazione di informazioni sensibili, la distruzione dei dati o l'accesso non autorizzato a risorse riservate.

La Cyber Kill Chain fornisce un quadro strategico per comprendere gli attacchi informatici e agire di conseguenza. Non esiste un approccio unico per affrontare un attacco, ma questo modello consente di mettersi nei panni dell'attaccante e di adottare un approccio simile per prevenire o mitigare l'intrusione. Nell'analisi di seguito vedremo le diverse fasi della Cyber Kill Chain nel dettaglio.



## RECONNAISSANCE

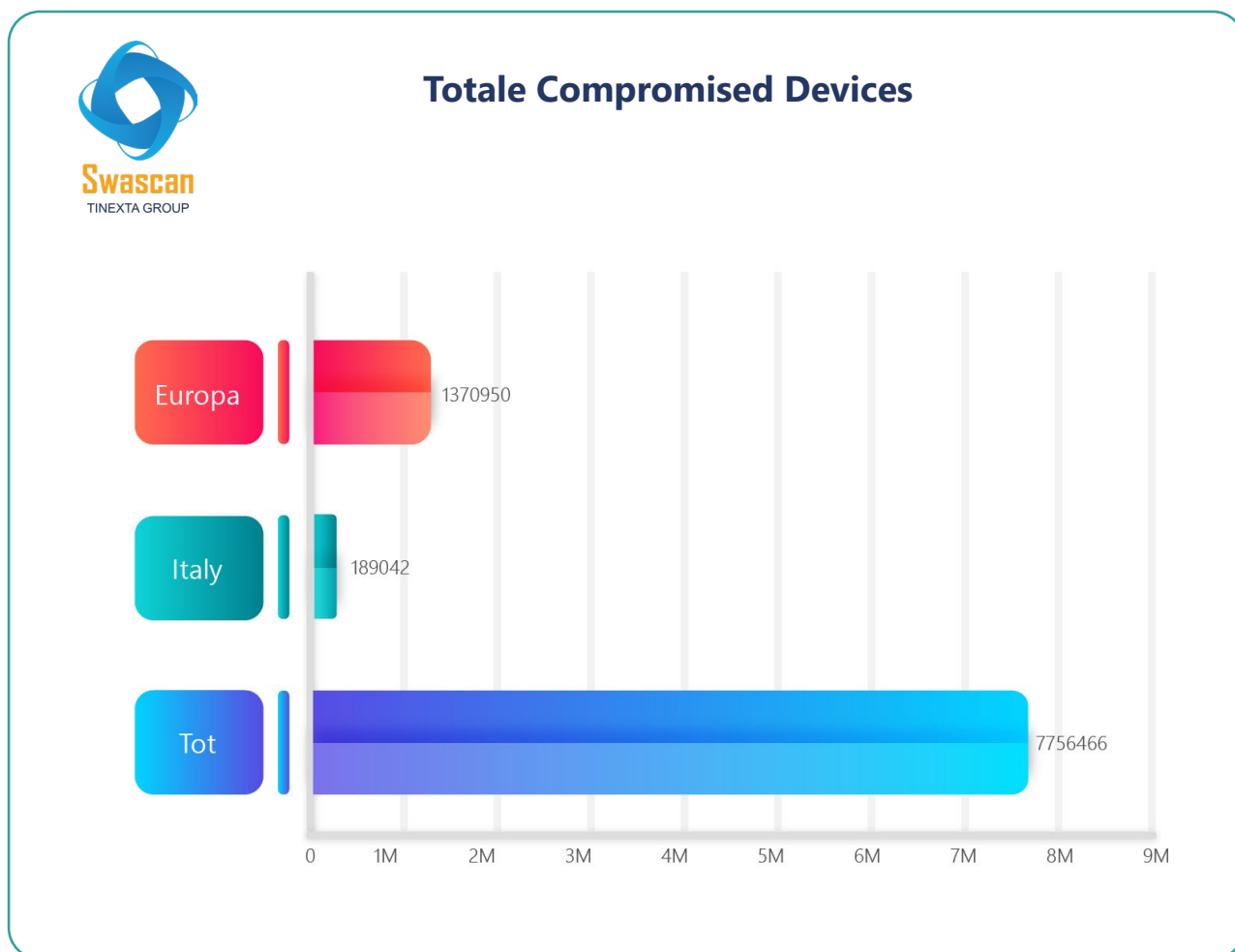


La fase di reconnaissance è la prima importante tappa all'interno della Cyber Kill Chain, durante la quale gli attaccanti raccolgono informazioni preziose per pianificare un attacco mirato. Durante questa fase, vengono adottate diverse strategie, tra cui, ad esempio, la raccolta di credenziali da mercati nel dark web, l'identificazione di nuove vulnerabilità (CVE) e l'utilizzo di campagne di social engineering.

Gli attaccanti possono acquisire credenziali sensibili da mercati nel Deep e Dark Web, dove vengono scambiate illegalmente informazioni rubate come username, password e dettagli di accesso a sistemi o account online. Queste credenziali possono provenire da violazioni dei dati precedenti o da tecniche di phishing e possono essere utilizzate per ottenere un accesso non autorizzato a sistemi o per impersonare un utente legittimo.

## Compromised devices, credential leaks & social engineering

Prendendo in riferimento due noti mercati di credenziali in vendita è stato rilevato un **totale di 7'756'466** dispositivi compromessi dai quali sono state esfiltrate credenziali che possono essere acquistate. In questo computo l'Italia presenta un **totale di 189'042** dispositivi compromessi.

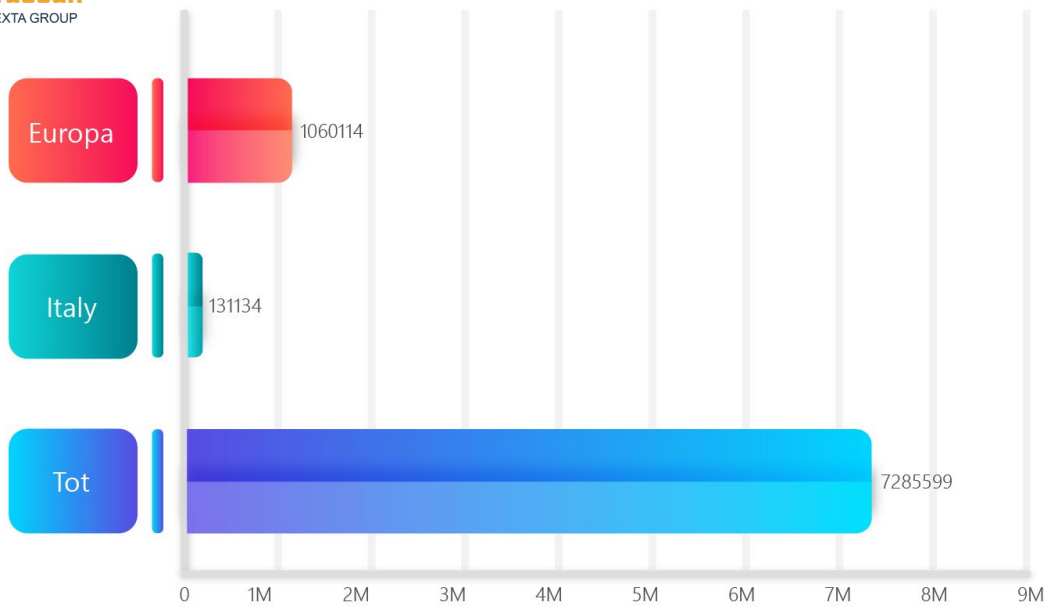


Da un'analisi approfondita del primo portale sono stati rilevati un totale di **7'285'599** dispositivi compromessi dai quali sono state esfiltrate credenziali di accesso. Facendo un focus sull'Europa, il totale è di **1'060'114** dispositivi compromessi di cui **131'134** italiani.





### Compromised Devices

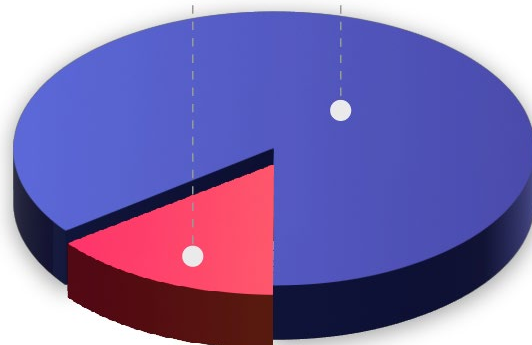


In riferimento al totale dei dispositivi compromessi l'Europa ricopre il **14,55% del totale** mentre l'Italia ricopre l'**1,8% del totale**.



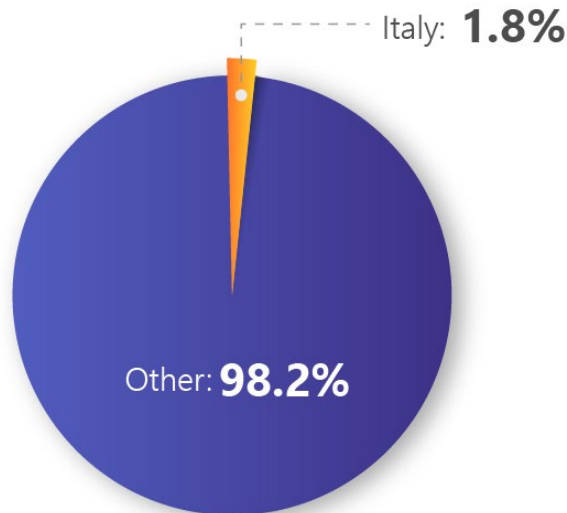
### Global vs Europe

EU: **14.5%**      Other: **85.5%**





### Global vs Italy

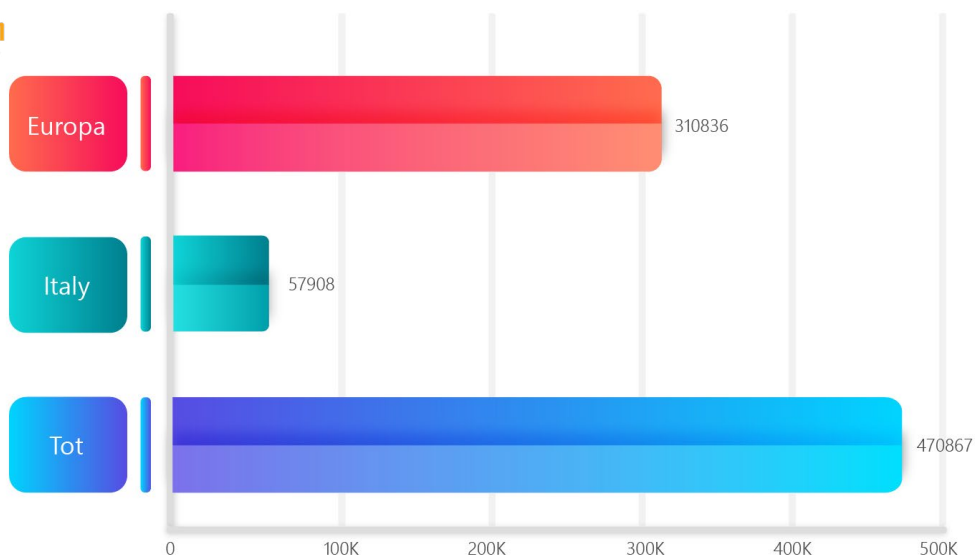


Il secondo portale in analisi invece presenta un totale di **470'867** dispositivi compromessi di cui **310'836 (66%) relativi all'Europa**.

Facendo un focus sull'Italia sono stati rilevati un totale di **57908 (12,3%)** dispositivi compromessi dal quale sono state esfiltrate credenziali.



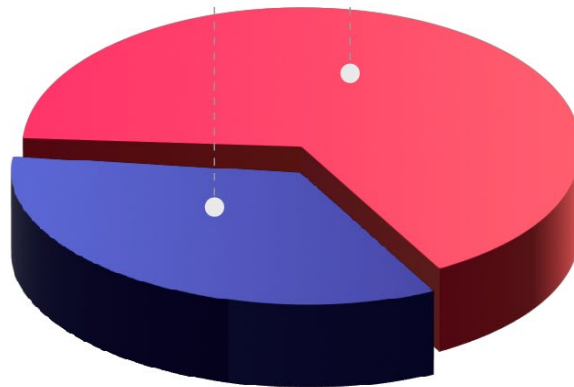
### TOT Compromised Devices





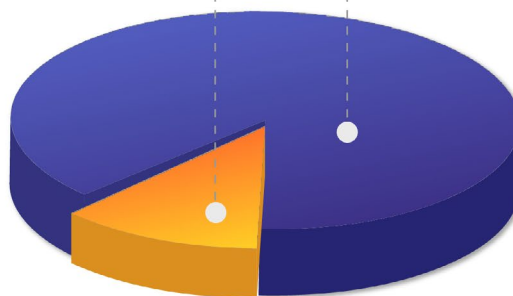
### Global vs Europe

Other: **34%** EU: **66%**



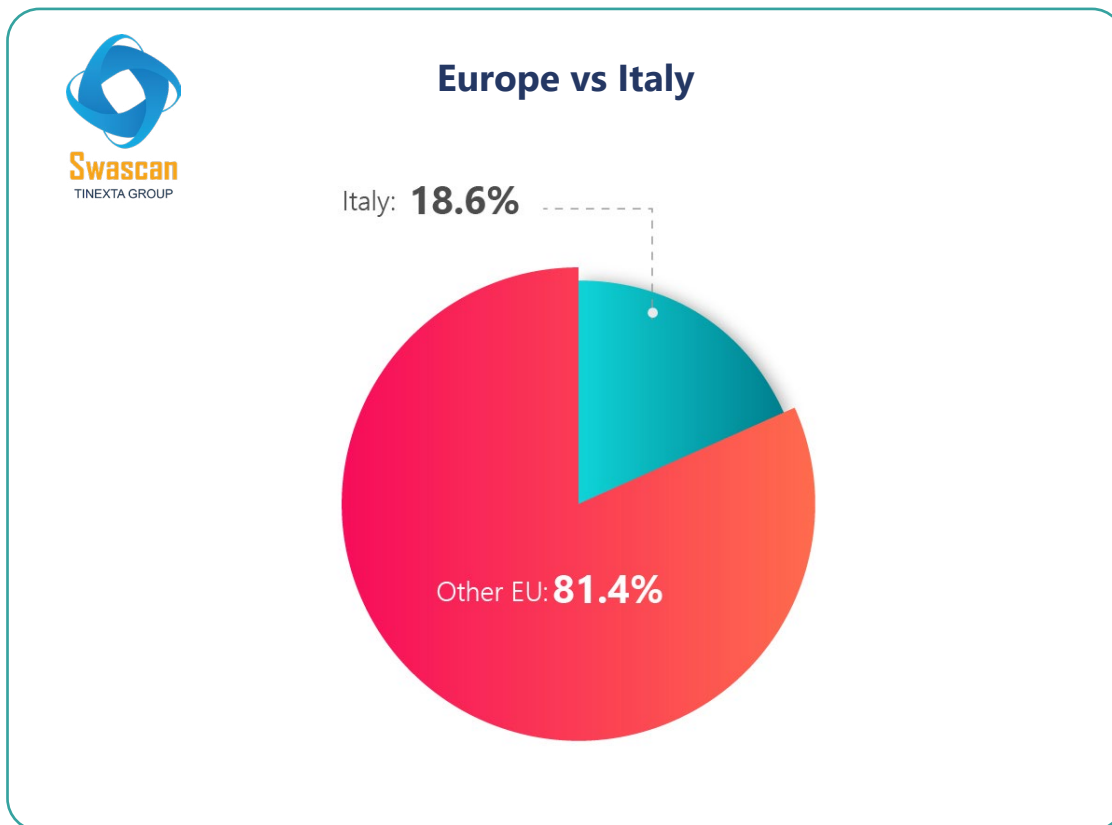
### Global vs Italy

Italy: **12.3%** other: **87.7%**





Tuttavia, in confronto all'Europa, l'Italia ricopre il **18,63%**.

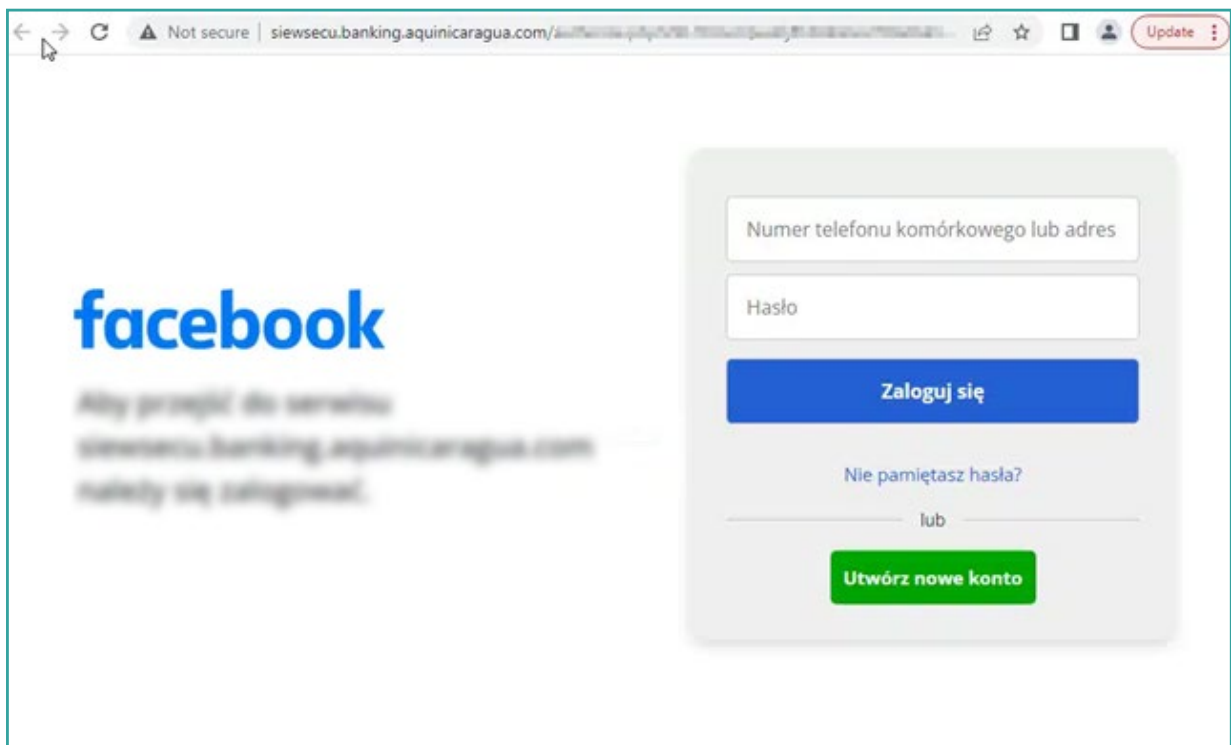
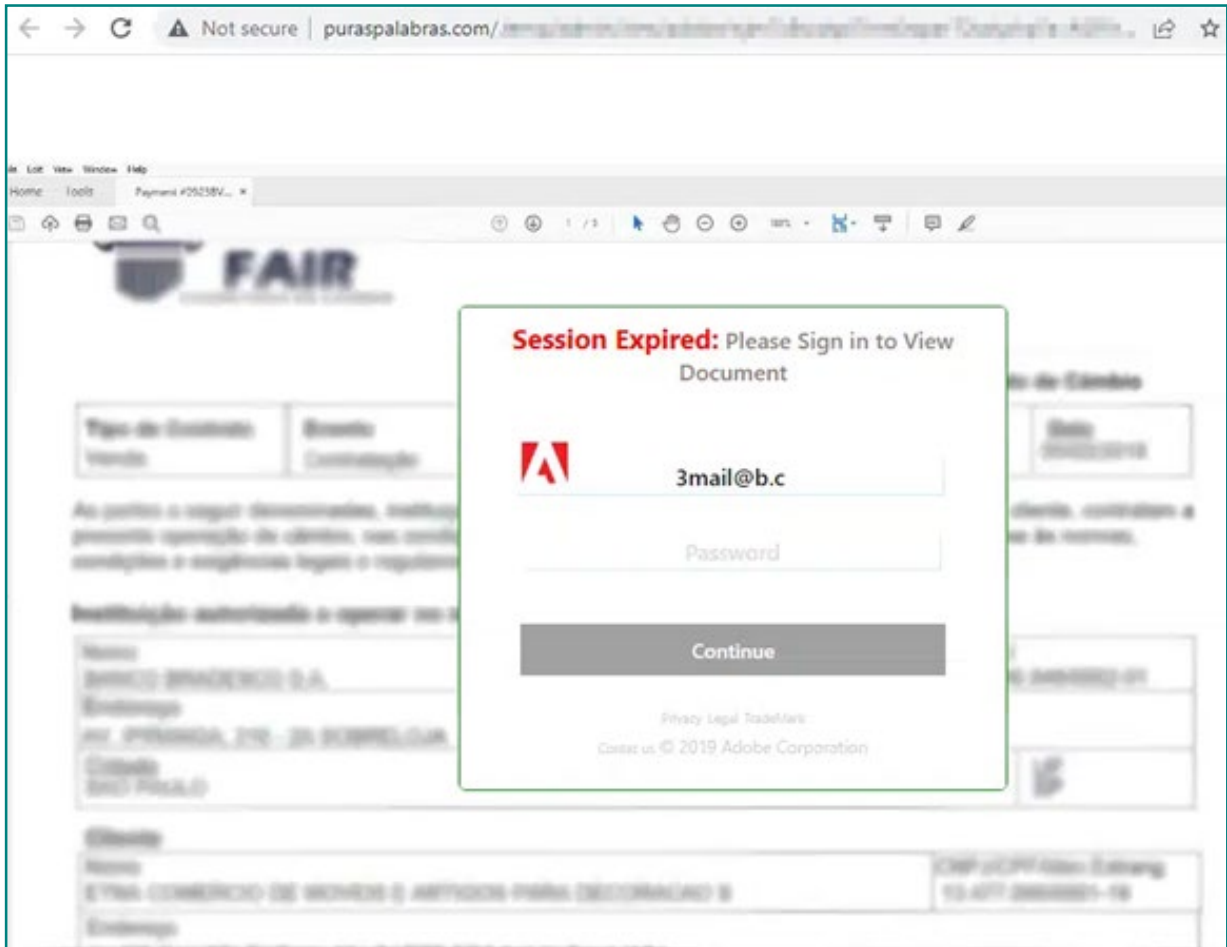


## Social engineering

---

Le campagne di social engineering costituiscono un'altra tattica comune nella fase di Reconnaissance. Gli attaccanti cercano di raccogliere informazioni preziose sugli utenti o sulle organizzazioni attraverso l'inganno e la manipolazione psicologica. Questo può coinvolgere l'invio di e-mail o messaggi di testo fraudolenti che richiedono informazioni sensibili o che inducono gli utenti a fare clic su link malevoli. Nel Q2 sono state osservate difatti **155'683 campagne di phishing**. Attraverso queste tattiche, gli aggressori cercano di ottenere accesso a informazioni confidenziali o di ingannare gli utenti per facilitare fasi successive dell'attacco.

Tra le campagne analizzate è possibile notare alcuni esempi dove si tenta di ingannare la vittima fingendosi prodotti o servizi reali:



Questo trend, secondo il CEO di Swascan, Pierguido Iezzi, mette in luce l'insidiosa e crescente minaccia relativa all'identità digitale di individui e imprese. Il mercato delle credenziali sottratte illegalmente è in forte ascesa, a riprova di quanto valore abbiano le nostre identità digitali negli ecosistemi del cybercrime, dove possono rapidamente essere monetizzati in molteplici modi, e della geopolitica, dove costituiscono uno strumento di cyberspionaggio a disposizione di chiunque. Il commercio delle identità digitali non è solo un campanello d'allarme per la sicurezza informatica, ma segnala infatti un'evoluzione verso la Guerra Cognitiva, in cui l'informazione e la conoscenza sono utilizzate come armi. Per le imprese, i governi e gli stati, questi attacchi rappresentano non solo un rischio per la sicurezza dei dati sensibili, ma possono erodere la fiducia dei cittadini e influenzare gravemente la reputazione e la sovranità. La sfumatura tra cybercrime e cyberwar diventa sempre più sottile, rendendo cruciale non solo l'educazione e l'investimento in soluzioni di sicurezza, ma anche una profonda riflessione da parte degli stati sul modello e sul governo della sfera cyber.

## Common Vulnerabilities and Exposures

---

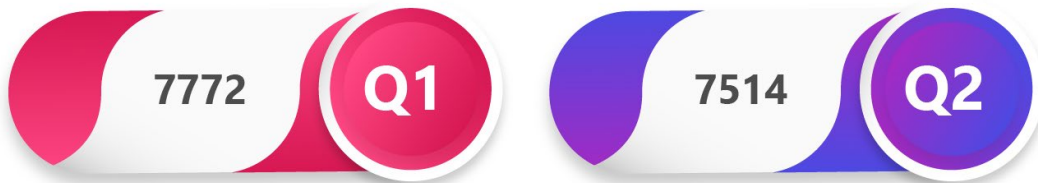
L'identificazione di nuove vulnerabilità, note come CVE (Common Vulnerabilities and Exposures), è un'altra componente critica della fase di Reconnaissance. Gli aggressori monitorano costantemente le nuove vulnerabilità che vengono scoperte nei software, nei sistemi operativi o nelle applicazioni. Questo permette loro di individuare i punti deboli nei sistemi bersaglio e di sfruttarli successivamente durante l'attacco.

Nel Q1 relativo al 2023 erano state pubblicate 7'772 nuove CVE contro le 7'514 pubblicate nel Q2:





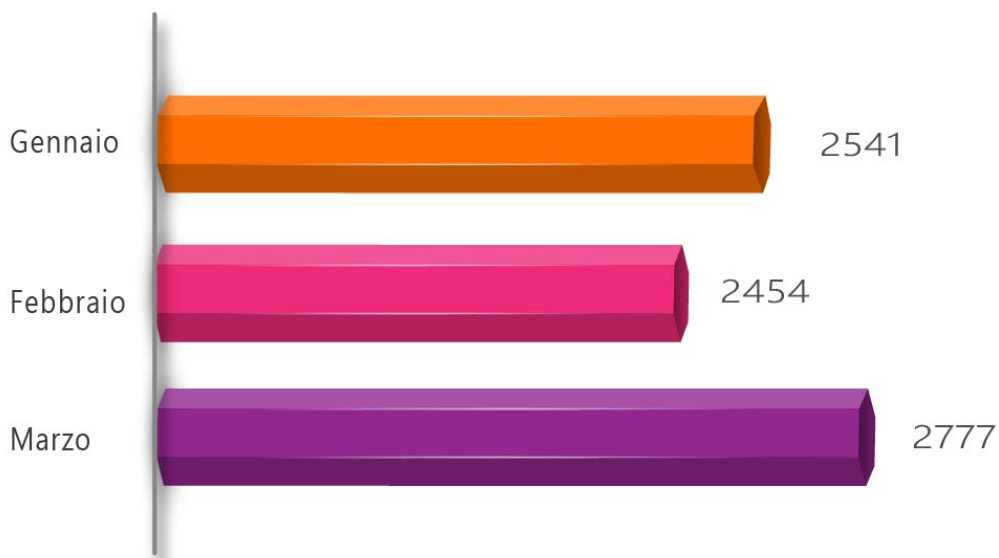
## CVE Q1 vs Q2 2023

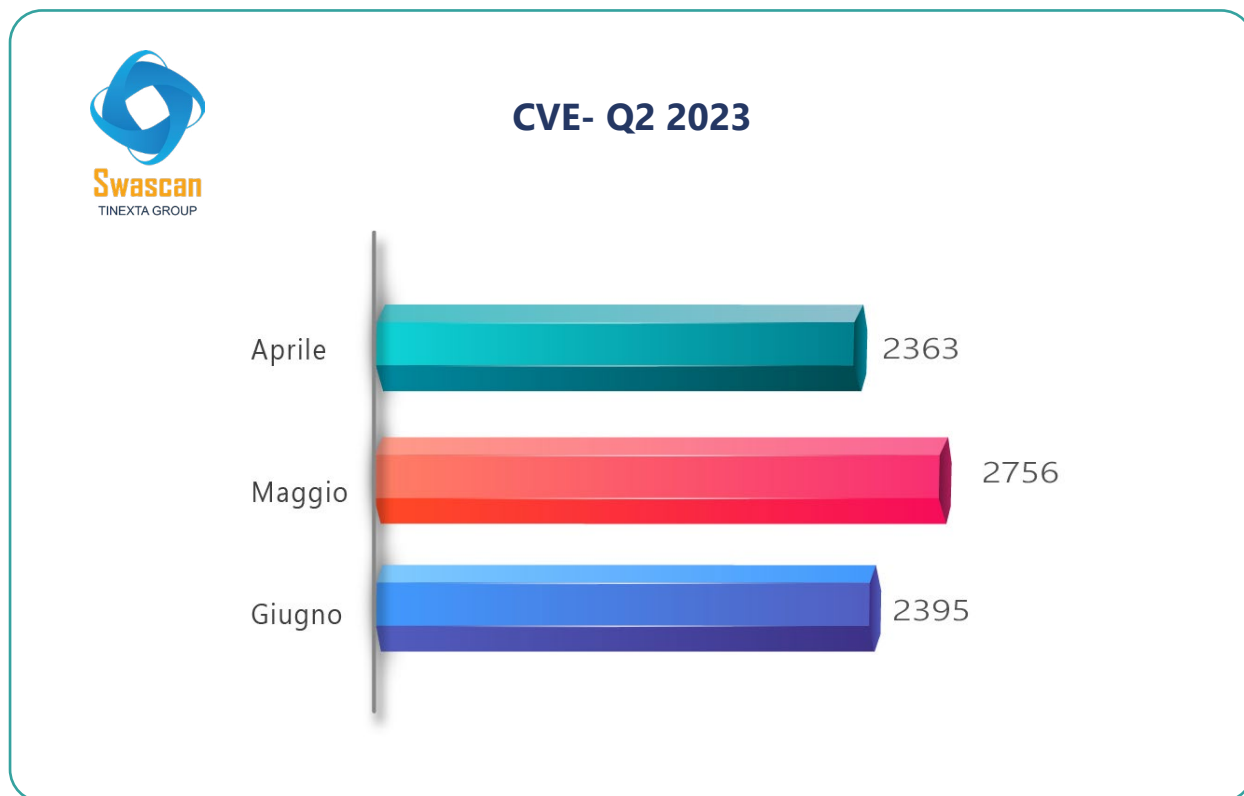


CVE - tracciate e segnalate dalla MITRE Corporation. Questo numero fa riferimento alle nuove vulnerabilità riconosciute e segnalate nel periodo in oggetto



## CVE- Q1 2023



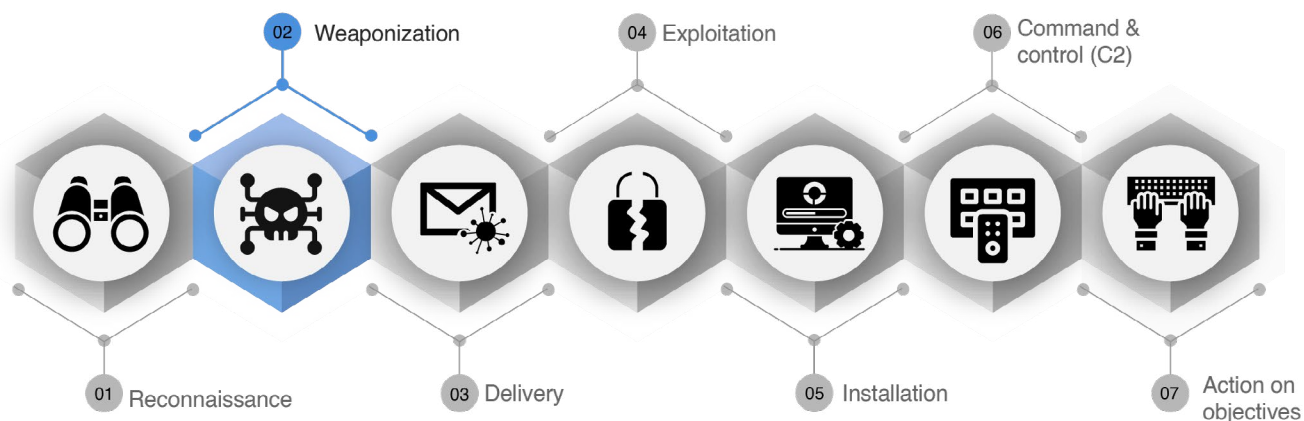


È possibile notare come solo nel mese di maggio siano state pubblicate 2'756 nuove CVE relative a vulnerabilità che potrebbero essere attenzionate e successivamente sfruttate da attaccanti.

Per proteggersi efficacemente dalla fase di Reconnaissance, le organizzazioni devono adottare diverse misure di sicurezza. Ciò include la vigilanza costante dei mercati nel dark web per monitorare eventuali violazioni dei dati aziendali, l'implementazione di soluzioni di rilevamento delle vulnerabilità per identificare e mitigare le nuove CVE, nonché la formazione e la consapevolezza degli utenti per riconoscere e resistere alle tattiche di social engineering.

Inoltre, è importante mantenere sistemi e applicazioni aggiornati con le ultime patch di sicurezza e adottare buone pratiche di sicurezza informatica, come l'utilizzo di password robuste e l'autenticazione a multi-fattori.

## WEAPONIZATION



La fase di weaponization è un'importante tappa all'interno della Cyber Kill Chain, in cui gli aggressori trasformano un payload malevolo in un'arma pronta per essere utilizzata contro il sistema target. Durante questa fase, vengono spesso veicolati diversi tipi di malware, tra cui botnet, info stealer e RAT.

**Le botnet** sono reti di computer compromessi e controllati da remoto dagli attaccanti. Questi bot possono essere utilizzati per condurre attacchi distribuiti di denial of service (**DDoS**), inviare spam o propagare ulteriormente il malware. L'attaccante sfrutta la botnet per inviare comandi ai bot compromessi e per ricevere informazioni raccolte da essi.

Gli infostealer sono tipi di **malware** progettati per rubare informazioni sensibili dai sistemi infettati. Questi malware possono raccogliere dati come credenziali di accesso, informazioni bancarie, dati di carte di credito o altre informazioni personali. Una volta raccolte, le informazioni vengono inviate al C2 dell'attaccante per un successivo sfruttamento o utilizzo a fini illeciti.

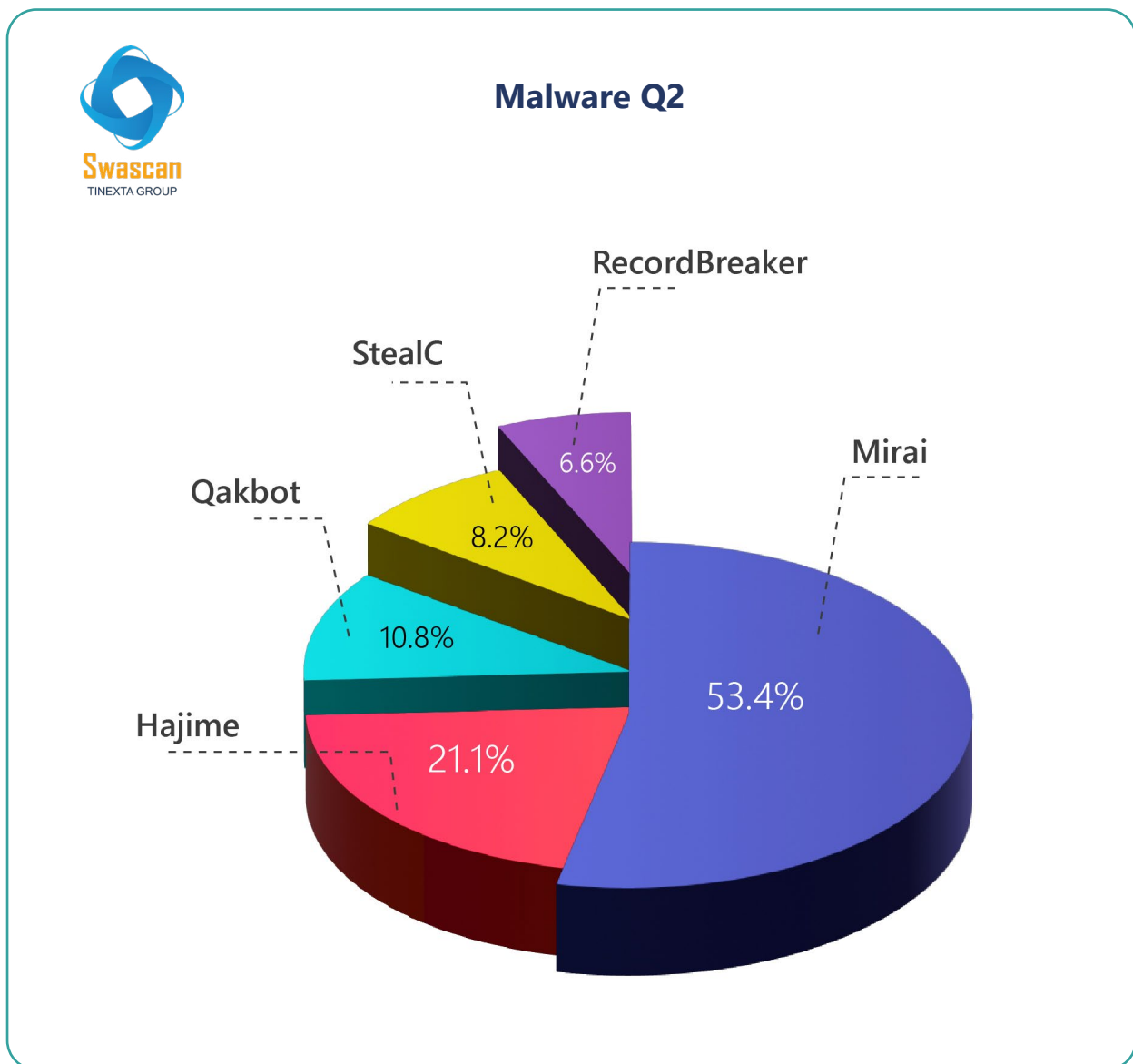
**I RAT**, ovvero i Trojan di accesso remoto, consentono agli aggressori di assumere il controllo completo del sistema compromesso da remoto. Gli attaccanti possono accedere al sistema, eseguire comandi, scaricare e installare ulteriori malware, esfiltrare dati o compiere altre azioni dannose. Questi strumenti offrono agli attaccanti un controllo furtivo e persistente sul sistema compromesso.

La fase di weaponization è cruciale per gli aggressori, poiché rappresenta il momento in cui il payload malevolo viene trasformato in uno strumento di attacco funzionante. Gli aggressori sfruttano queste forme di malware, come botnet, infostealer e RAT, per ottenere e mantenere l'accesso non autorizzato al sistema bersaglio e per condurre ulteriori fasi dell'attacco informatico.



## Malware

Il SOC & Threat Intelligence Team di Swascan ha identificato i malware più diffusi durante questo periodo: al primo posto **Mirai** che ha rappresentato il **53.4%** dei malware veicolati mentre al secondo e terzo posto **Hajime** e **Qakbot** con rispettivamente **21.1%** e **10.8%**.



Da notare come Qakbot risulti ad oggi ampiamente utilizzato in particolar modo da gang Ransomware nella fase di Weaponization per eseguire payload malevoli che portano spesso all'esecuzione del Ransomware stesso.

## DELIVERY



Una delle minacce più diffuse e dannose rilevate nel Q2 è il phishing, un attacco informatico che mira a ingannare gli utenti e a ottenere accesso non autorizzato alle loro informazioni.

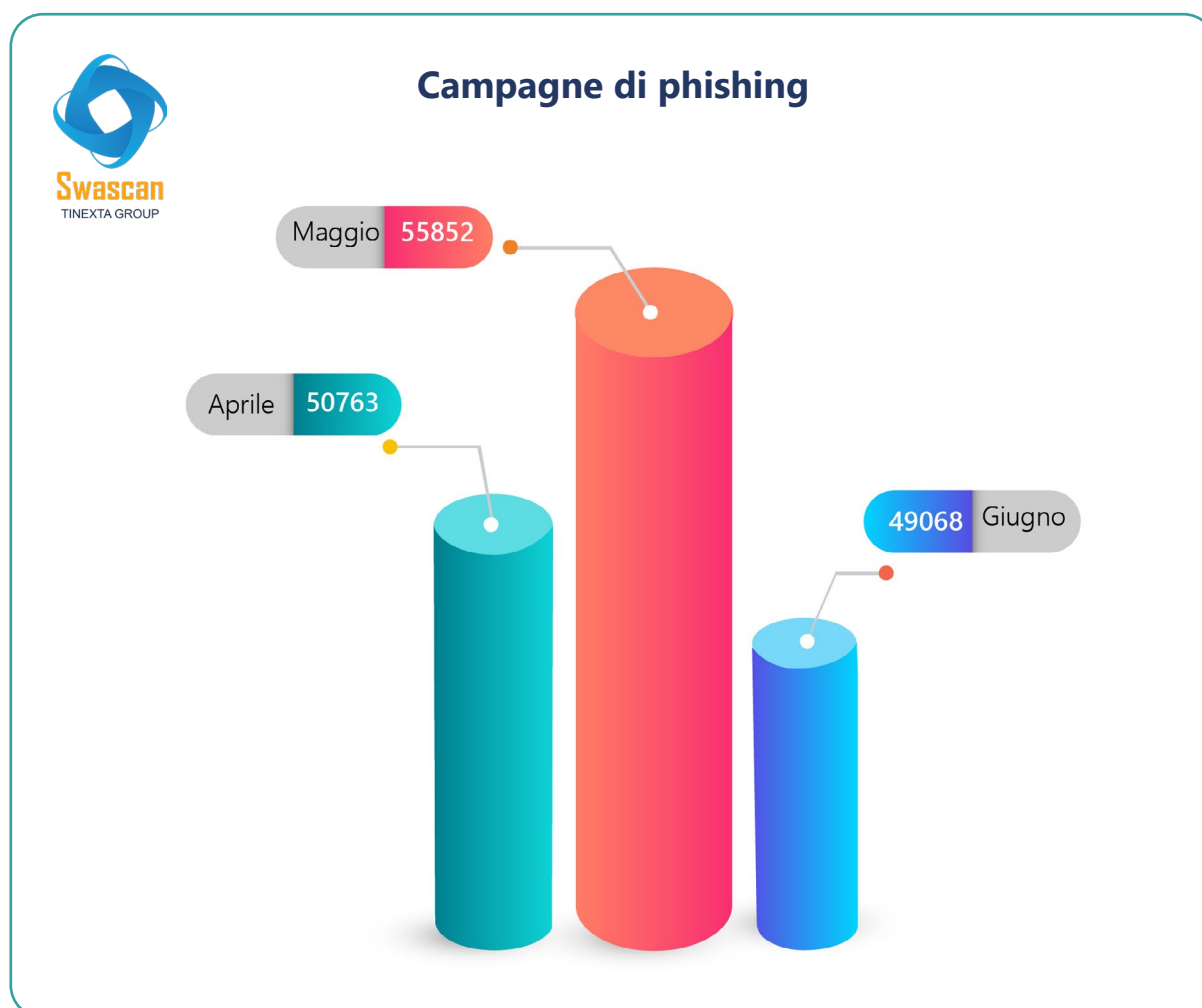
Nel contesto della Cyber Kill Chain il phishing si colloca nella fase di "Delivery" o consegna.

La fase di delivery rappresenta il momento in cui l'attaccante consegna un payload o un meccanismo di attacco all'utente prescelto. Il phishing, in particolare, sfrutta tecniche sofisticate per inviare e-mail, messaggi di testo o comunicazioni ingannevoli che sembrano provenire da fonti attendibili o legittime. Gli aggressori cercano di ingannare gli utenti persuadendoli a fare clic su link malevoli, scaricare allegati infetti o rivelare informazioni riservate.

## Phishing

Il trend del phishing è in continua evoluzione e adattamento alle nuove tecnologie e alle strategie di difesa messe in atto dagli esperti di sicurezza. Gli attaccanti si avvalgono di metodi sempre più sofisticati, come l'utilizzo di tecniche di social engineering mirate e l'imitazione accurata di siti web e comunicazioni autentiche, al fine di trarre in inganno le vittime e indurle a compiere azioni che potrebbero compromettere la loro sicurezza.

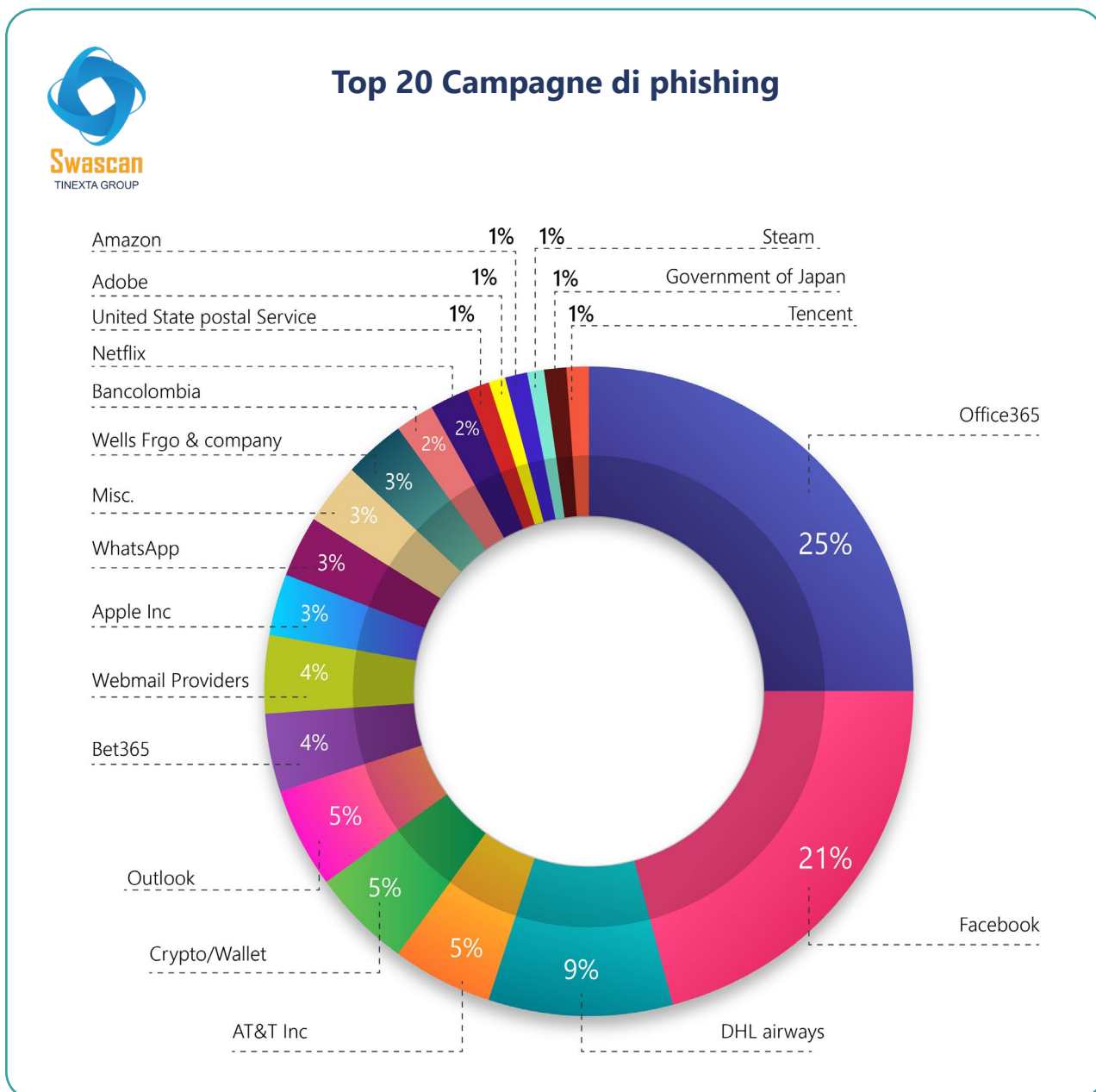
Sono state quindi rilevate nel secondo trimestre un **totale di 155'683** campagne di phishing così distribuite:



Dai tre mesi in analisi sono state estrapolate le top 20 campagne di phishing con il relativo tema della campagna.

- » Nel mese di **aprile** sono state rilevate **50'763** campagne e, di queste, 14'507 sono state identificate come Spear Phishing mentre 24'117 sono relative ai top 20 brand imitati.
- » Nel mese di **maggio** sono state rilevate **55'852** campagne e, di queste, 15'778 sono state identificate come Spear Phishing mentre 28'170 sono relative ai top 20 brand imitati.
- » Mentre nel mese di **giugno** sono state rilevate un totale di **49'068** campagne. Di queste, 12'141 sono state identificate come Spear Phishing mentre 25'842 sono relative ai top 20 brand imitati.

Di seguito invece la percentuale relativa al tema della campagna nel secondo trimestre:



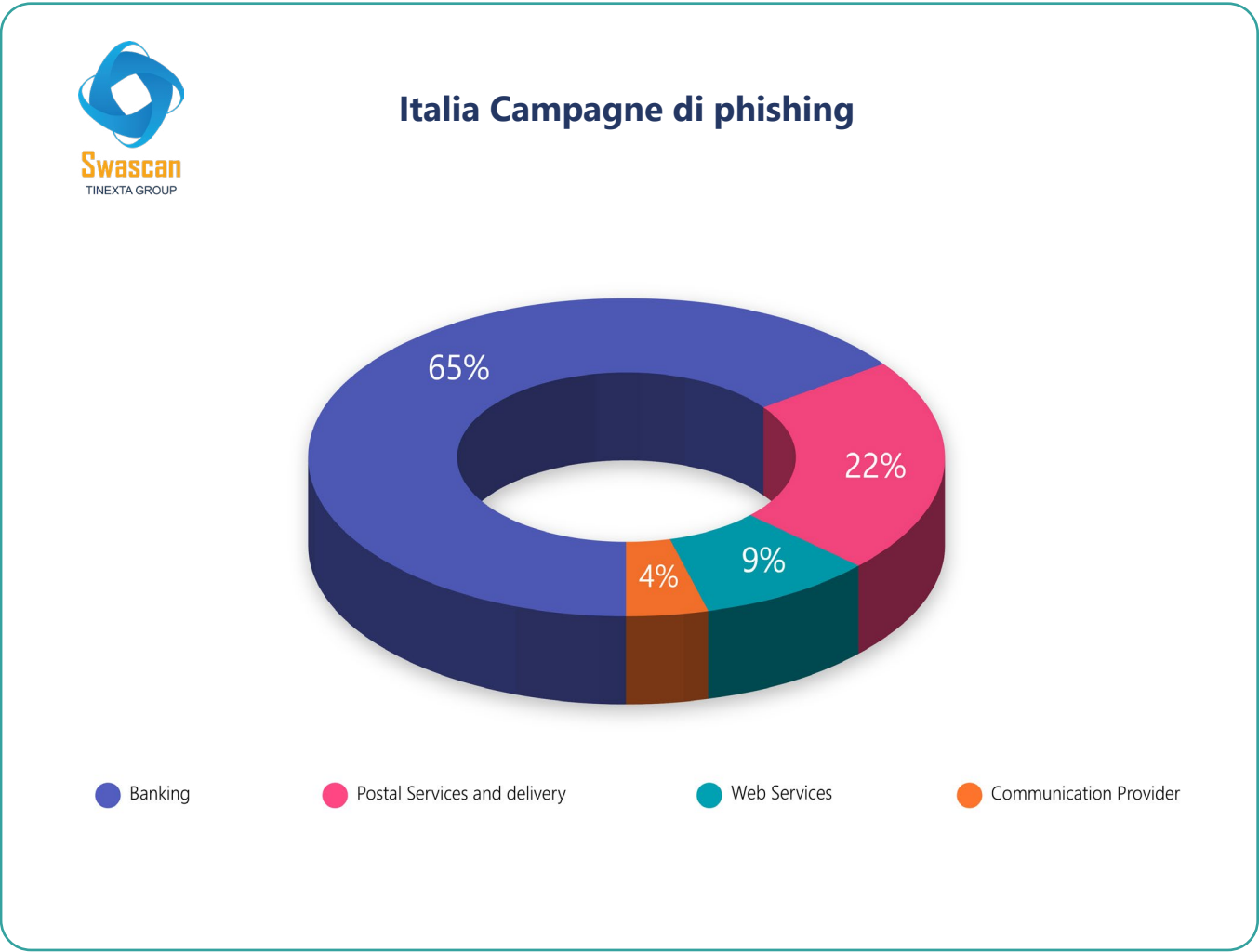


Al primo posto c'è Office365, con il 25% degli attacchi di phishing, seguito da Facebook, con il 21%. Queste campagne vengono spesso utilizzate come esca per la cattura di credenziali e furto di account social.

Al terzo posto c'è DHL con il 9%, spesso sfruttato dagli hacker per creare e-mail contraffatte che sembrano legittime, convincendo le vittime a fornire le loro informazioni personali.

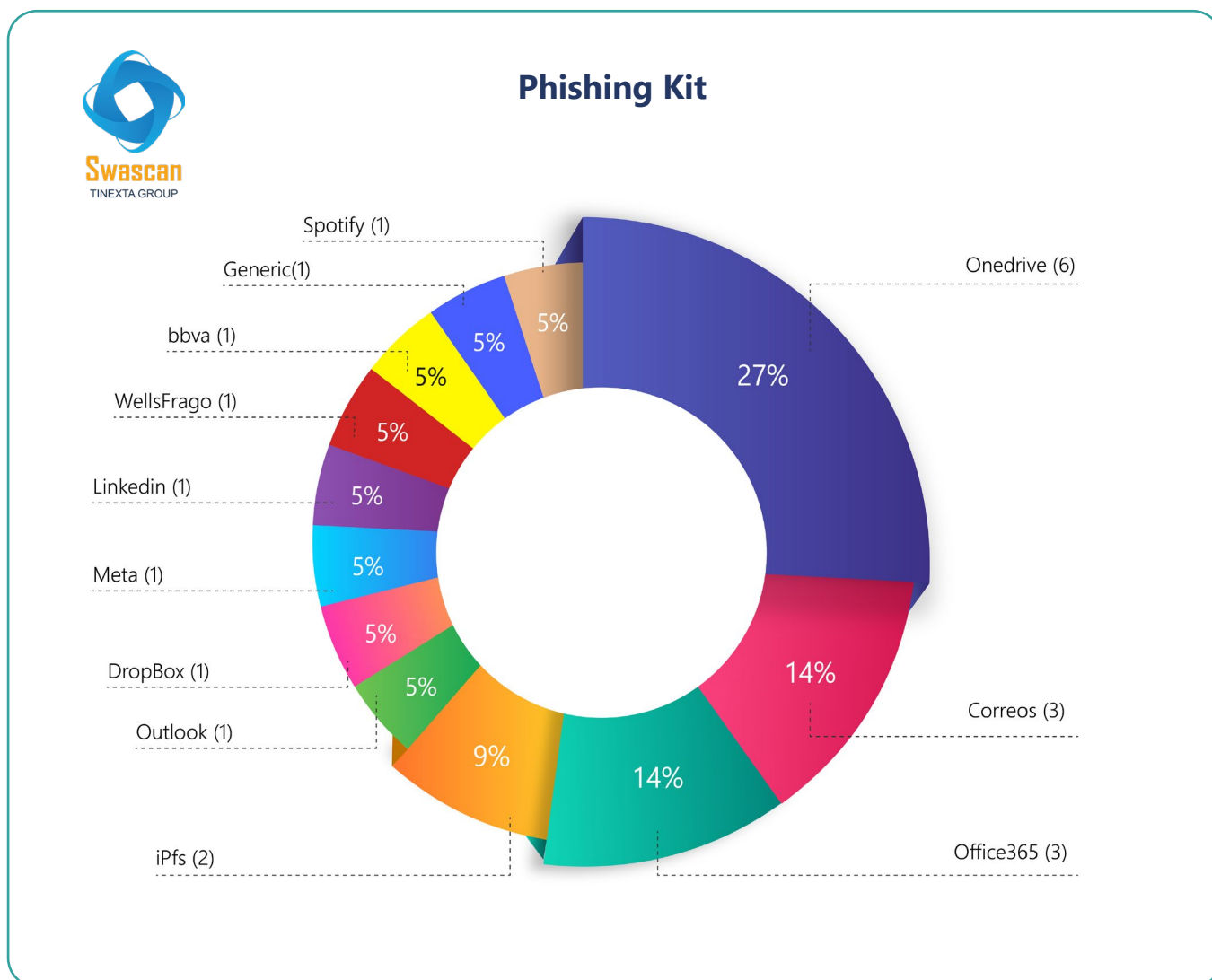
Il resto della lista include AT&T Inc. (5%), Crypto/Wallet (5%), Outlook (5%), Bet365 (4%), Webmail Providers (4%), Apple Inc. (3%), WhatsApp (3%), Wells Fargo & Company (3%), Misc. (3%), Bancolombia (2%), Netflix (2%), United States Postal Service (1%), Adobe Inc. (1%), Amazon (1%), Steam (1%), Government of Japan (1%) e Tencent (1%).

Facendo un focus sulle campagne che hanno invece interessato **l'Italia**, sono state rilevate nel Q2 un **totale di 959 campagne** che hanno imitato i brand dei seguenti settori:



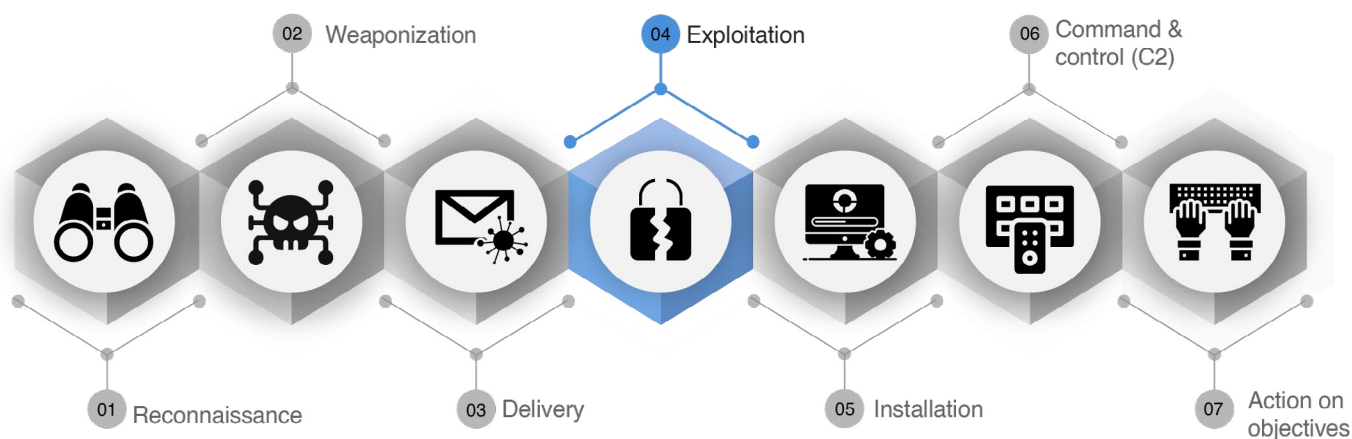
È possibile notare come il settore bancario sia quello maggiormente preso di mira dagli attaccanti con lo scopo di esfiltrare credenziali di accesso ed informazioni di pagamento.

Sono inoltre stati rilevati **22 Phishing Kit** nel trimestre in analisi dove è possibile notare come i temi principali risultino spesso legati a servizi Microsoft (OneDrive, Outlook, Office365), bancari e Social.



Tali phishing kit vengono spesso impiegati massivamente per campagne mirate alla cattura di informazioni sensibili (credenziali, carte di credito) o al deploy di malware che possono variare da Information Stealer a Remote Access Trojan, con questi ultimi che possono poi rivelarsi il vettore di attacco iniziale per campagne Ransomware.

## EXPLOITATION



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

Nel contesto della Cyber Kill Chain, un modello utilizzato per comprendere e affrontare gli attacchi cibernetici e lo sfruttamento di CVE si colloca nella fase di "Exploitation".

La fase di Exploitation rappresenta uno dei momenti cruciali all'interno della Cyber Kill Chain, durante il quale gli attaccanti cercano di sfruttare una vulnerabilità o una falla nel sistema bersaglio per ottenere un accesso non autorizzato. È il passaggio successivo alla fase di delivery, in cui il payload malevolo viene consegnato all'utente o all'ambiente target.

Durante la fase di Exploitation, gli aggressori sfruttano una serie di tecniche sofisticate per approfittare di vulnerabilità nei software, nei sistemi operativi o nelle configurazioni di rete. Queste vulnerabilità possono essere il risultato di errori di programmazione, di patch mancanti o di configurazioni inadeguate, lasciando spazio per l'ingresso dell'attaccante.

Gli attaccanti possono utilizzare diverse metodologie per portare avanti l'exploit. Ad esempio, possono avvalersi di exploit di tipo "zero-day", che sfruttano vulnerabilità precedentemente sconosciute e non ancora patchate dai fornitori di software. Oppure possono utilizzare exploit noti ma che non sono stati ancora corretti da parte degli utenti o delle organizzazioni.

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

## CVE

Di seguito le CVE più discusse e sfruttate dai Threat Actor e relative al Q2 2023:

CVE ID	Summary	CVSScore
CVE-2023-34362	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.	9.8
CVE-2023-27997	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.	9.2
CVE-2023-2868	A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product affecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.	9.8



CVE-2023-2982	<p>The WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 7.6.4. This is due to insufficient encryption on the user being supplied during a login validated through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they know the email address associated with that user. This was partially patched in version 7.6.4 and fully patched in version 7.6.5.</p>	9.8
CVE-2023-33299	<p>A deserialization of untrusted data in Fortinet FortiNAC below 7.2.1, below 9.4.3, below 9.2.8 and all earlier versions of 8.x allows attacker to execute unauthorized code or commands via specifically crafted request on inter-server communication port. Note FortiNAC versions 8.x will not be fixed.</p>	9.8
CVE-2023-28424	<p>Soko if the code that powers packages.gentoo.org. Prior to version 1.0.2, the two package search handlers, `Search` and `SearchFeed`, implemented in `pkg/app/handler/packages/search.go`, are affected by a SQL injection via the `q` parameter. As a result, unauthenticated attackers can execute arbitrary SQL queries on `https://packages.gentoo.org/`. It was also demonstrated that primitive was enough to gain code execution in the context of the PostgreSQL container. The issue was addressed in commit `4fa6e4b619c0362728955b6ec56eab0e0cbf1e23y` of version 1.0.2 using prepared statements to interpolate user-controlled data in SQL queries.</p>	9.8
CVE-2023-32434	<p>An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 8.8.1, iOS 16.5.1 and iPadOS 16.5.1, iOS 15.7.7 and iPadOS 15.7.7, macOS Big Sur 11.7.8, macOS Monterey 12.6.7, macOS Ventura 13.4.1, watchOS 9.5.2. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.</p>	7.8
CVE-2023-32435	<p>A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 16.4, iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3, iOS 15.7.7 and iPadOS 15.7.7. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.</p>	8.8

CVE-2023-20887	Aria Operations for Networks contains a command injection vulnerability. A malicious actor with network access to VMware Aria Operations for Networks may be able to perform a command injection attack resulting in remote code execution.	9.8
CVE-2023-32031	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8

Lo 0-Day relativo alla CVE-2023-34362, ad esempio, è stato attivamente sfruttato dalla gang Ransomware CI0p portando il gruppo alla compromissione di oltre 150 organizzazioni tra cui compagnie del settore consulting, technology, energy ed ha portato alla compromissione stimata di dati personali di oltre 16 milioni di persone.

## COMMAND & CONTROL



Nel secondo trimestre del 2023, i malware continuano a rappresentare una minaccia per la sicurezza informatica di aziende e individui in tutto il mondo.

Nel contesto della Cyber Kill Chain, l'installazione di Malware per la comunicazione con un server remoto si colloca nella fase di "Command&Control".

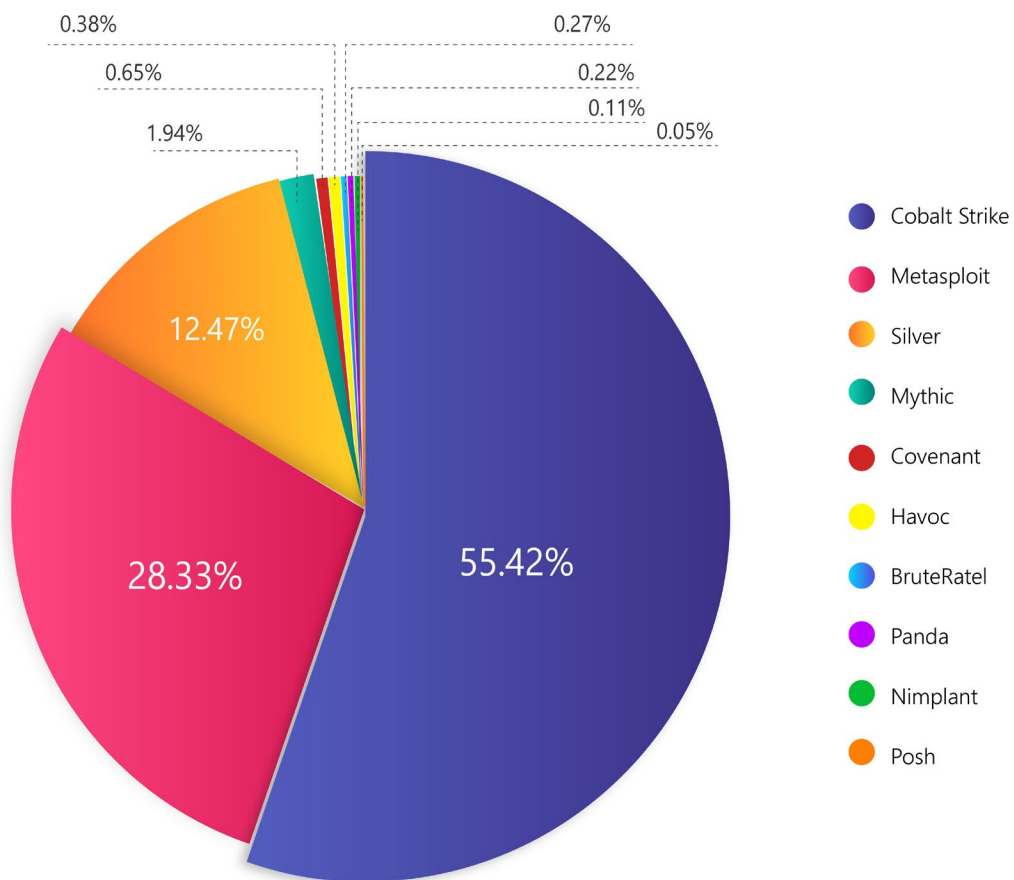
La fase di **Command & Control ("C2")** è cruciale per gli attaccanti, poiché consente loro di mantenere il controllo sulle macchine compromesse e di continuare a eseguire operazioni malevole senza essere rilevati. È essenziale che le organizzazioni implementino soluzioni di rilevamento delle minacce avanzate per identificare e bloccare la comunicazione tra i sistemi compromessi e gli attaccanti.

Durante la fase di C2, gli aggressori utilizzano una varietà di tecniche e strumenti per mantenere il controllo sul sistema compromesso e interagire con esso. Questo coinvolge l'uso di malware sofisticati e framework di Command & Control.

Il SOC & Threat Intelligence Team di Swascan ha identificato i Framework più diffusi durante questo periodo:



## I Framework più diffusi



Al primo posto troviamo CobaltStrike, che ha rappresentato il 55,42% dei Framework C2 utilizzati mentre al secondo e terzo posto troviamo Metasploit e Silver con rispettivamente 28,33% e 12,47%.



## ACTIONS ON OBJECTIVES



Nel Q2 2023 si è registrato un significativo aumento delle vittime colpite da attacchi ransomware, con un **totale di 1'451 incidenti** segnalati in tutto il mondo ed un **aumento del 62%** rispetto al trimestre precedente. Si tratta dell'ultima fase della Cyber Kill Chain, conosciuta come "Actions on Objectives", che rappresenta il momento culminante di un attacco. Una volta infiltratosi con successo nel sistema bersaglio, l'attaccante è in grado di agire per raggiungere il suo obiettivo iniziale. Le azioni intraprese in questa fase possono assumere molteplici forme, che vanno dall'estrapolazione di dati sensibili fino alla completa distruzione degli stessi.

Le vittime del ransomware nel secondo trimestre provengono da un'ampia gamma di paesi e isole, raggiungendo un totale di 89 paesi coinvolti. Questo dimostra come il ransomware sia un problema globale che non conosce confini geografici: le organizzazioni e gli individui di tutto il mondo sono stati bersaglio di attacchi, mettendo a rischio la sicurezza dei dati e la continuità operativa.

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 Q2 2023.

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

LockBit	Alphav/BlackCat	8Base	CLOP	BlackBasta
PLAY	BianLian	Royal	Akira	SiegedSec
Medusa	Snatch	Nokoyawa	BlackByte	Rhysida

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

## Attacchi ransomware

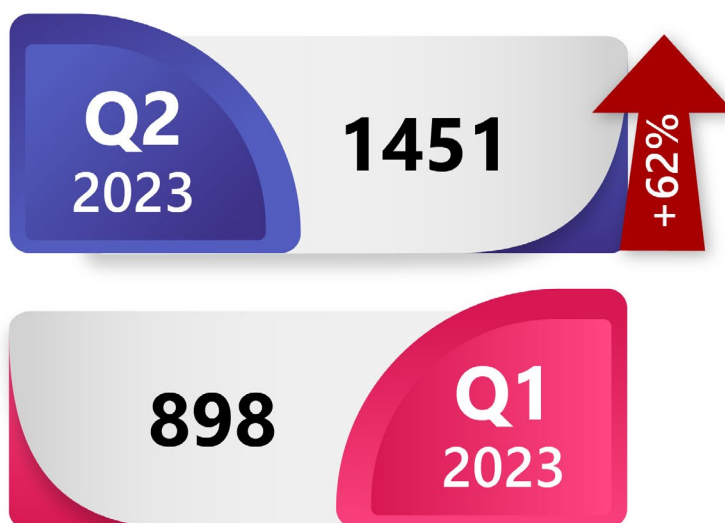
Il periodo compreso tra il primo trimestre (Q1) e il secondo trimestre (Q2) del 2023 ha visto un significativo aumento degli attacchi ransomware in tutto il mondo. Durante il **Q1**, erano state identificate un totale di **36 diverse gang di ransomware**, che avevano colpito numerosi settori e aziende in tutto il globo. La regione più colpita era quella degli Stati Uniti, con un elevato numero di attacchi segnalati.

Tuttavia, il **Q2** ha visto un ulteriore aumento degli attacchi ransomware, con un totale di **43 gruppi identificati**. La regione degli Stati Uniti continua ad essere la più colpita, ma è stato registrato un incremento del numero di paesi del mondo interessati dagli attacchi, che **sono saliti da 79 (Q1) a 89 (Q2)**. Questo suggerisce un'espansione delle operazioni di attacco da parte delle gang di ransomware, che stanno prendendo di mira una gamma sempre maggiore di paesi.

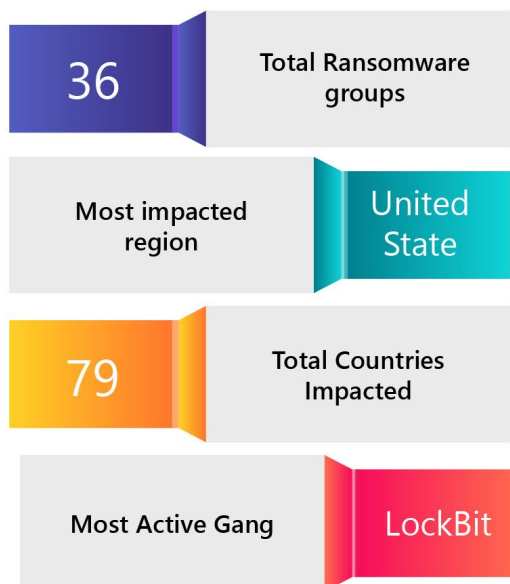
Tra tutti i gruppi di ransomware attivi durante il Q2, LockBit è rimasto il più prolifico e aggressivo, operando su larga scala e colpendo numerose organizzazioni in tutto il mondo.



Numero di Target colpiti dalle gang con data leak.  
**Confronto Q1 2023 e Q2 2023**



## Q1 2023



## Q2 2023



Analizzando il Q2 2023, si riscontrano:

1. **+183%** di vittime dall'inizio dell'anno
2. **Il mese di maggio** ha registrato un forte aumento degli attacchi ransomware, con un totale di **575 attacchi** registrati. Ciò rappresenta un **incremento del 51%** rispetto ad aprile e del 228% rispetto a gennaio.
3. **Aumento** delle vittime rispetto al Q2 2022 del **105%**

Durante il trimestre considerato, il numero di attacchi ransomware è aumentato in modo significativo. Nel dettaglio, durante il mese di aprile, sono stati registrati **381 attacchi** ransomware, e, rispetto al mese precedente, si è verificato un **aumento del 58%** nel numero di attacchi.

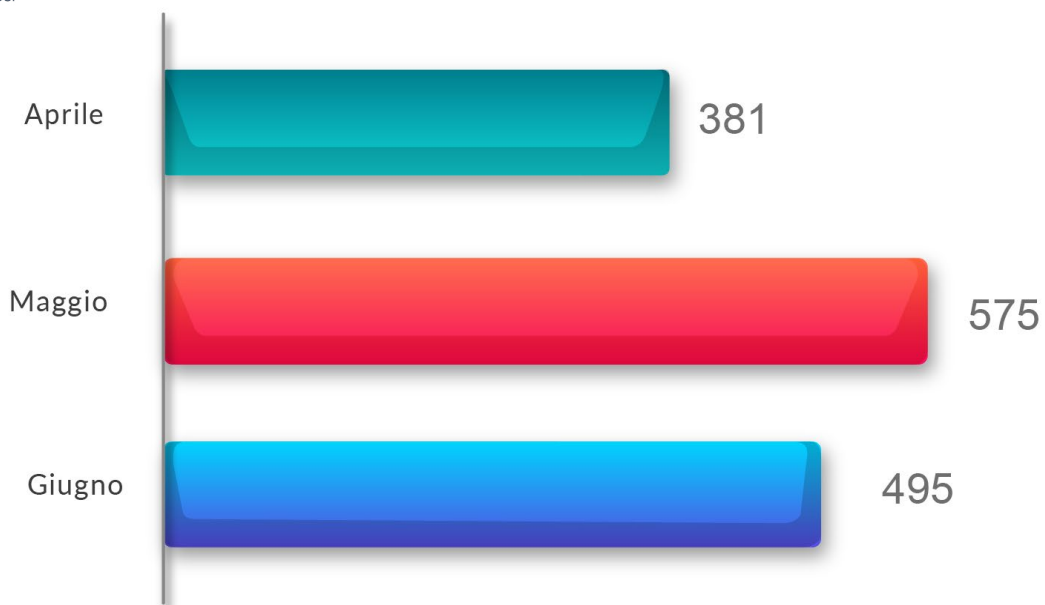
Nel mese di maggio, il numero di attacchi ransomware è aumentato ulteriormente, raggiungendo **un totale di 575** attacchi registrati. Questo rappresenta un incremento del 51% rispetto ad aprile. L'aumento significativo del numero di attacchi conferma la tendenza preoccupante e l'urgente necessità di adottare misure di sicurezza efficaci.

Anche nel mese di giugno, gli attacchi ransomware sono rimasti elevati, con un totale di **495 attacchi** registrati. Nonostante una leggera diminuzione rispetto al mese precedente, **l'aumento del 30%** rispetto ad aprile evidenzia la persistente minaccia di questa forma di attacco informatico.





### Q2 2023

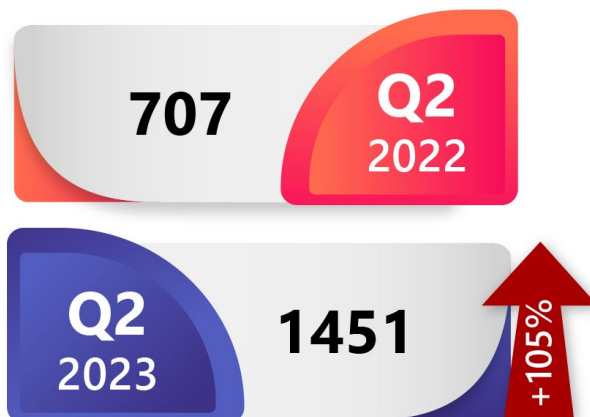


Inoltre, comparando il Q2 2022 e il Q2 2023 si riscontra un aumento di attacchi del **105%**:



Numero di Target colpiti dalle gang con data leak.

### Confronto Q2 2022 e Q2 2023



La minaccia degli attacchi ransomware continua infatti ad evolversi a un ritmo preoccupante con un'esplosione di attività criminali nel secondo semestre del 2023. Confrontando i dati del 2022 e del 2023, emerge una tendenza allarmante che richiede azioni decisive per mitigare i danni e proteggere le organizzazioni da gravi conseguenze. I dati raccolti rivelano, infatti, un netto aumento degli attacchi ransomware in tutti i mesi del 2023 rispetto allo stesso periodo dell'anno precedente. A partire da gennaio, si è registrato un incremento significativo degli attacchi, passando da 112 nel 2022 a 175 nel 2023. Questa tendenza è proseguita anche nei mesi successivi, con Febbraio che ha registrato un aumento da 200 a 266, marzo da 232 a 457 e aprile da 298 a 381.

Tuttavia, è nel mese di maggio che si evidenzia uno degli incrementi più preoccupanti. Mentre nel 2022 gli attacchi ransomware erano stati di 223, nel 2023 il numero è salito fino a 575, rappresentando un aumento di oltre il doppio rispetto all'anno precedente. Giugno, l'ultimo mese preso in considerazione, ha confermato questo rialzo allarmante, passando da 187 attacchi nel 2022 a 495 nel 2023.

### H1 2022 vs H1 2023

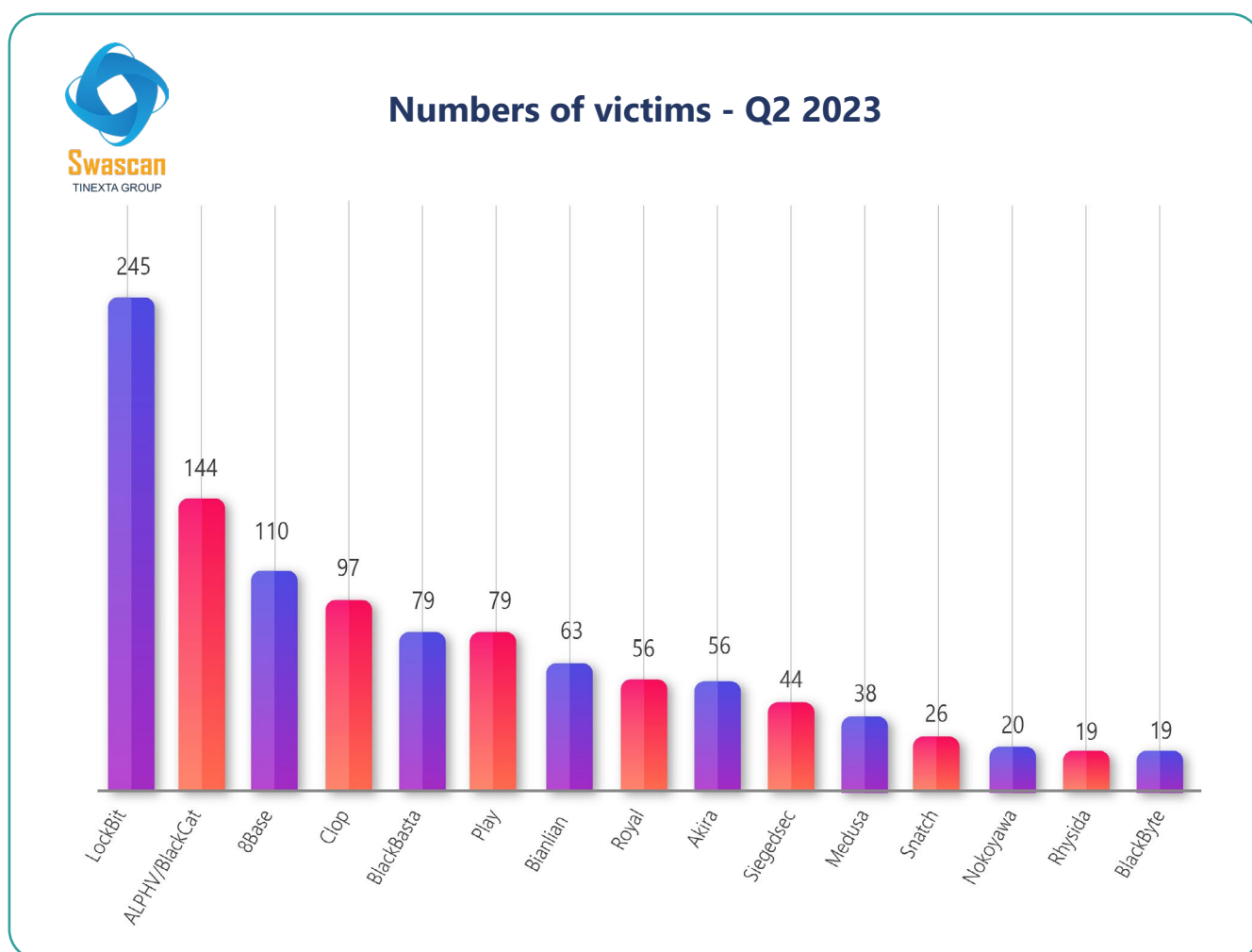


## Le gang ransomware più prolifiche

**LockBit** si conferma la gang più prolifica nel panorama degli attacchi ransomware, con ben **245 attacchi** registrati nel Q2 2023. Un'altra gang che ha attirato l'attenzione è **Alphv/BlackCat**, responsabile di **144 attacchi** ransomware nel trimestre analizzato. Anche 8Base si è distinta per la sua aggressività, colpendo un totale di 110 organizzazioni.

Emersa di recente, la gang ransomware Akira ha già colpito diverse vittime, di cui la maggior parte localizzate negli Stati Uniti. Queste vittime appartengono ad una varietà di settori, come BAFSI (Banche, Assicurazioni, Finanza e Servizi Immobiliari), Costruzioni, Educazione, Sanità, settore Manifatturiero e altri, sottolineando come nessun settore sia al sicuro da queste minacce digitali.

Akira non è l'unica nuova gang del trimestre che si classifica nella top 15: la gang ransomware Rhysida è stata osservata per la prima volta a Maggio del 2023, e si è assicurata un posto tra le prime 15.



Nel frattempo, la gang di ransomware **8Base** sta mirando ad organizzazioni in tutto il mondo con attacchi di doppia estorsione, ottenendo un flusso costante di nuove vittime sin dall'inizio di giugno. La gang è apparsa per la prima volta a **Marzo** del 2022, rimanendo relativamente silenziosa, con pochi attacchi di rilievo. Tuttavia, nel mese di **giugno 2023**, l'operazione ransomware ha registrato un **aumento significativo** dell'attività, prendendo di mira numerose aziende in diverse **industrie**.

## Distribuzione geografica globale delle vittime

---

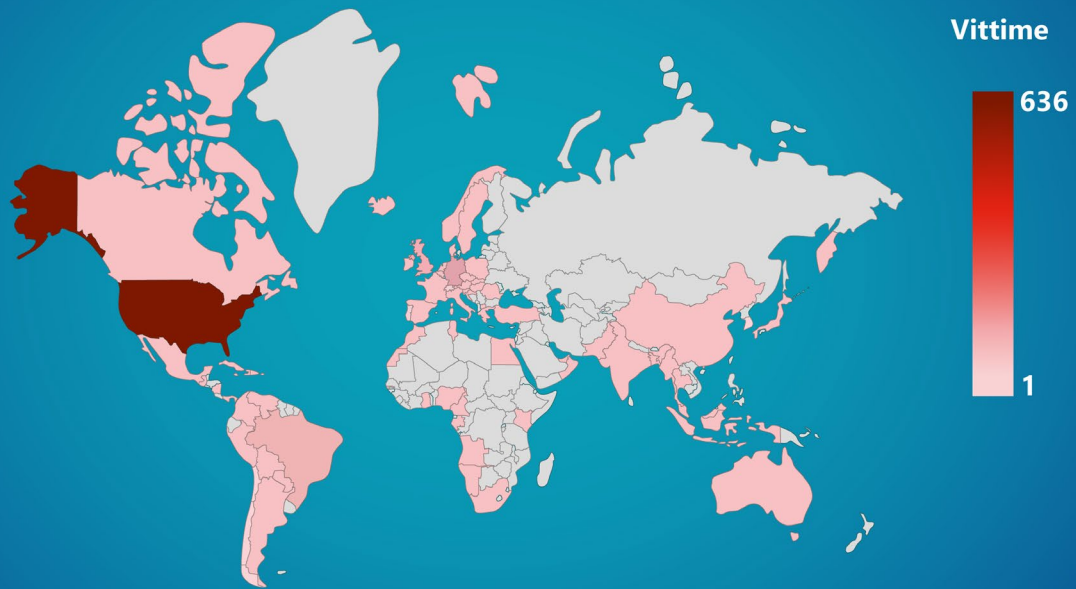
L'aumento degli attacchi ransomware nel secondo trimestre del 2023 ha avuto un impatto significativo su numerose aziende in tutto il mondo: gli **Stati Uniti** sono risultati essere **il paese più colpito**, con ben **636 aziende vittime** di ransomware nel periodo considerato.








Il Regno Unito e il Canada, con rispettivamente 69 e 60 aziende che hanno subito attacchi ransomware. La Germania, con 54 aziende colpite, si posiziona anch'essa tra i paesi più colpiti da ransomware nel secondo trimestre. Seguono la Francia con 39 aziende, il Brasile con 38, l'Italia con 35 e la Spagna con 28. I paesi europei citati hanno sperimentato un aumento significativo rispetto al trimestre precedente, evidenziando l'allarmante tendenza di diffusione di questi attacchi anche al di fuori del primato mantenuto dagli Stati Uniti.

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

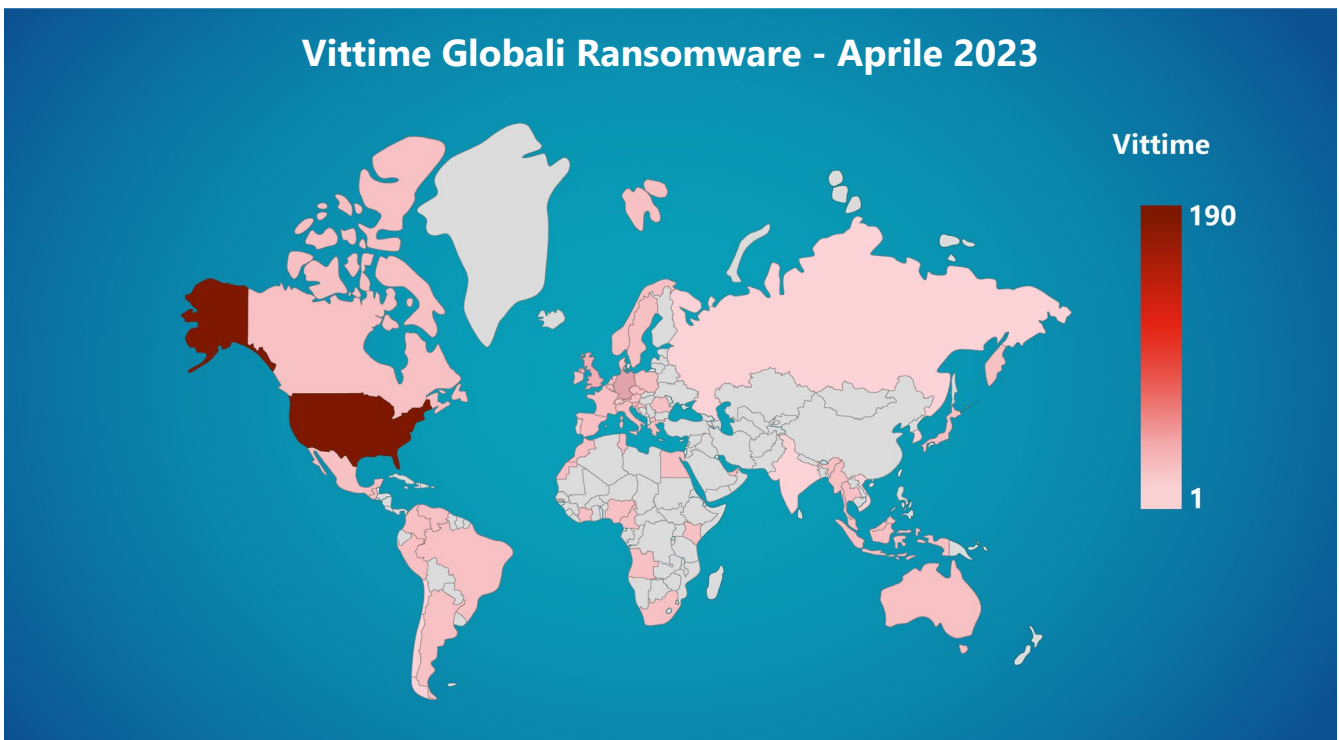


## Vittime Globali Ransomware - Q2 2023



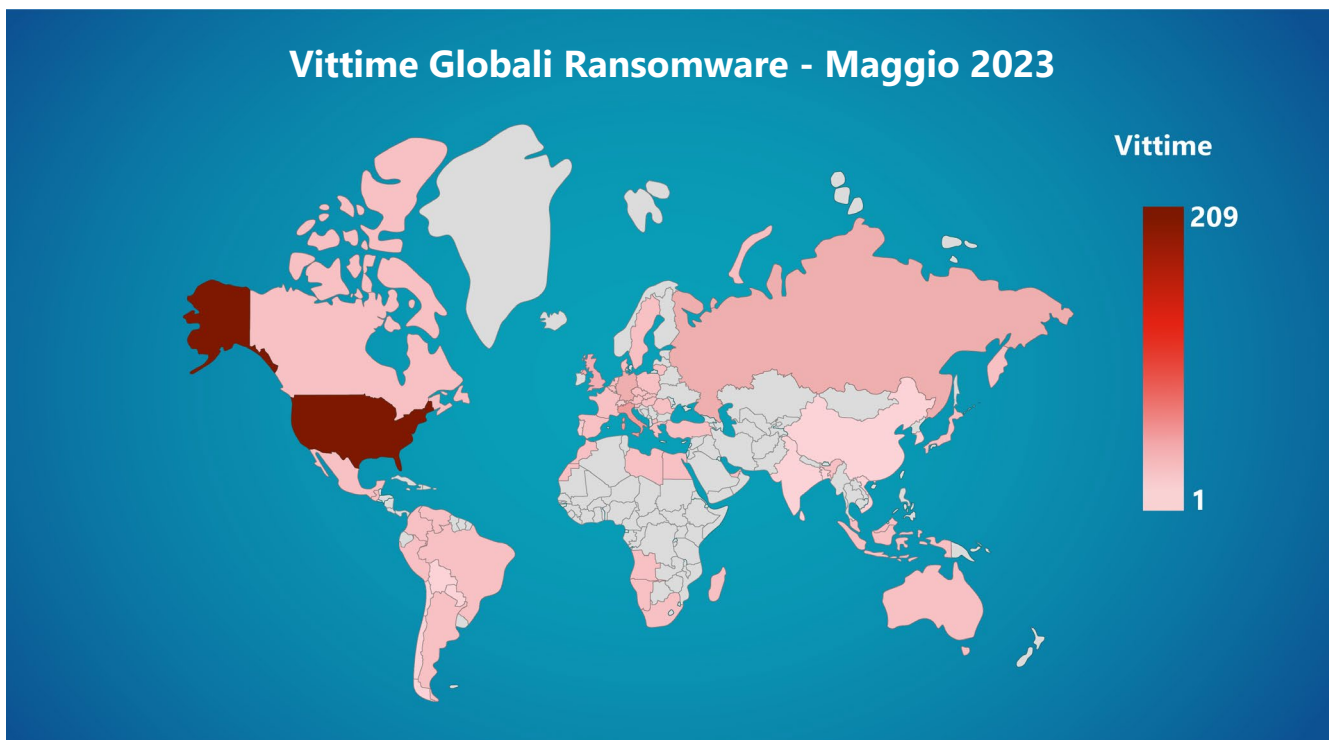
PAESE		Numero di aziende vittime di Ransomware con dati pubblicati – Q2 2023
	United States	636
	United Kingdom	69
	Canada	60
	Germany	54
	France	39
	Brazil	38
	Italy	35
	Spain	28

Nel mese di aprile si contano un totale di 56 paesi attaccati, con 190 vittime negli Stati Uniti. Nello stesso mese, in Italia il numero di aziende colpite è 9.



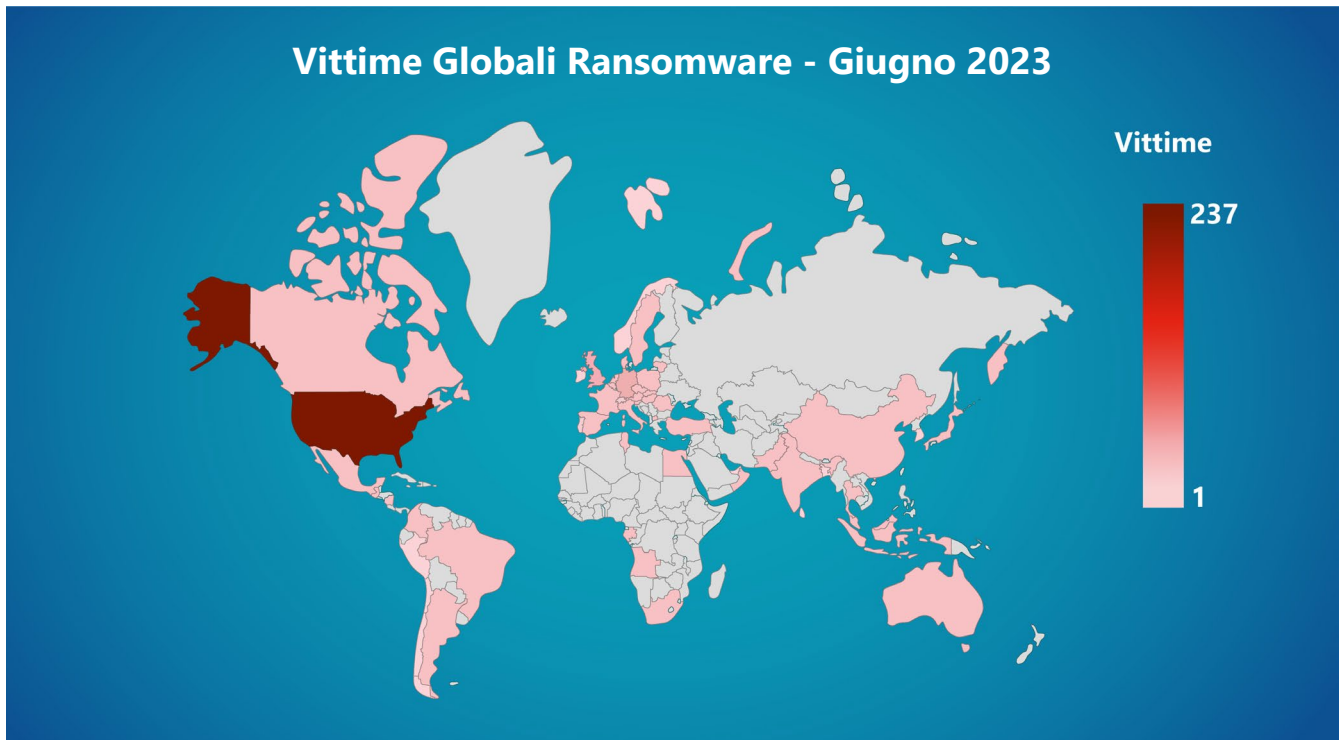
PAESE		Numero di aziende vittime di Ransomware con dati pubblicati – aprile 2023
	United States	190
	Canada	18
	Germany	17
	France	13
	United Kingdom	13
	Brazil	9
	Italy	9
	Australia	8



Stesso discorso per il mese di maggio, in cui gli Stati Uniti contano un totale di 209 vittime. Salgono anche le vittime in Italia, per un totale di 17 nel mese preso in analisi.



PAESE		Numero di aziende vittime di Ransomware con dati pubblicati – maggio 2023
	United States	209
	Russia	53
	United Kingdom	30
	Canada	27
	Germany	22
	Italy	17
	Spain	14
	Brazil	13

Anche a giugno 2023 il più alto numero di vittime è riscontrato negli Stati Uniti (237). Nello stesso mese, in Italia se ne contano 12.



<b>PAESE</b>		<b>Numero di aziende vittime di Ransomware con dati pubblicati – giugno 2023</b>
	United States	237
	United Kingdom	26
	Colombia	17
	Brazil	16
	Canada	15
	Germany	15
	Switzerland	15
	France	14

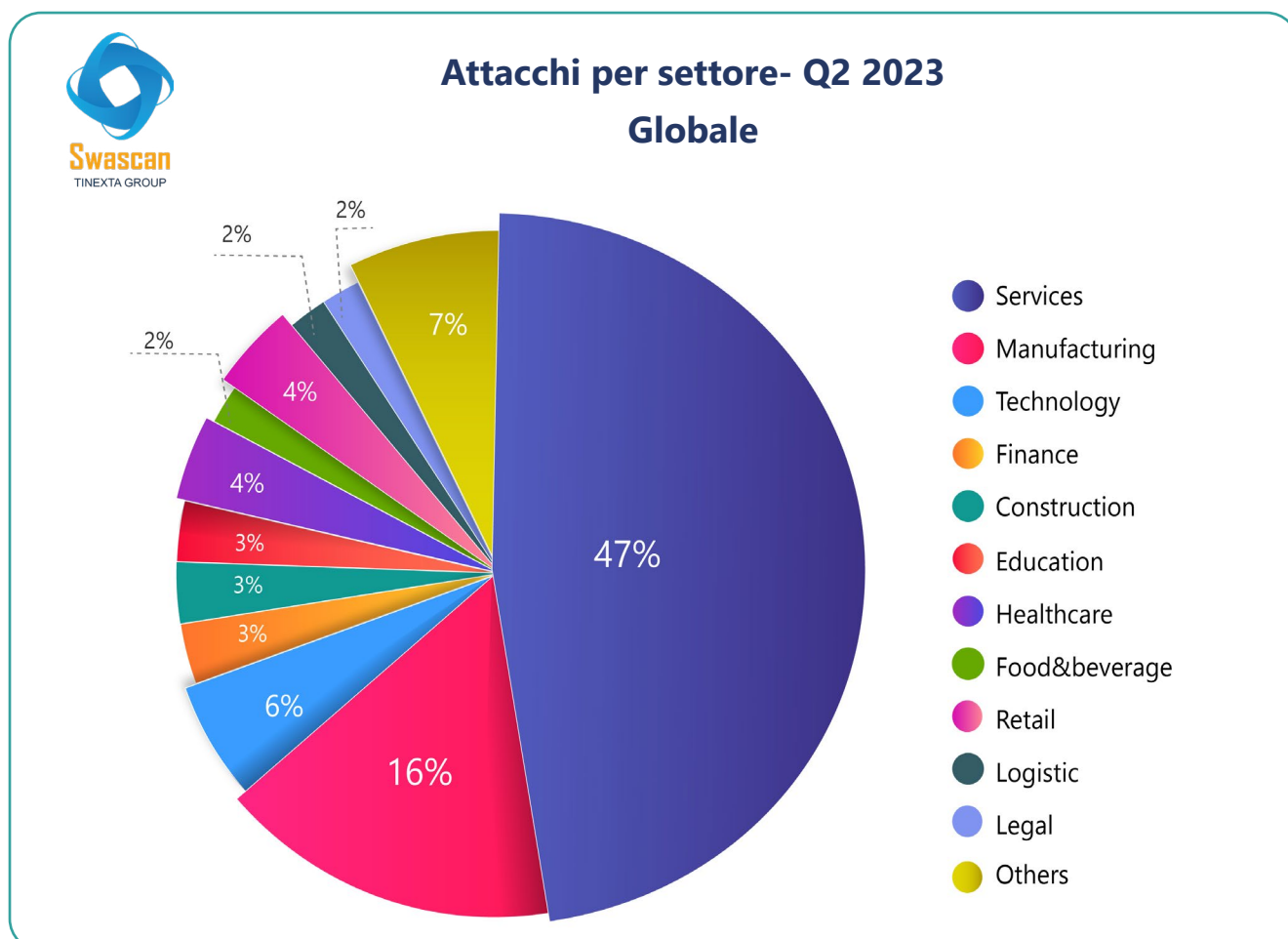


## I settori presi di mira dalla minaccia ransomware

Durante il secondo trimestre del 2023, gli attacchi ransomware hanno avuto un impatto significativo su diversi settori industriali. Tra i settori più colpiti, il settore dei servizi ha registrato il numero più elevato di vittime. Il settore manifatturiero è stato anch'esso duramente colpito, con un impatto significativo sulla produzione, la catena di approvvigionamento e la sicurezza dei dati aziendali. Il settore tecnologico, nonostante sia tradizionalmente più attento alla sicurezza informatica, ha registrato diverse aziende vittime di ransomware nel periodo considerato. Questo evidenzia la sofisticazione e la persistenza degli attacchi, che sono riusciti a superare le difese anche delle aziende considerate ipoteticamente più tecnologicamente avanzate.

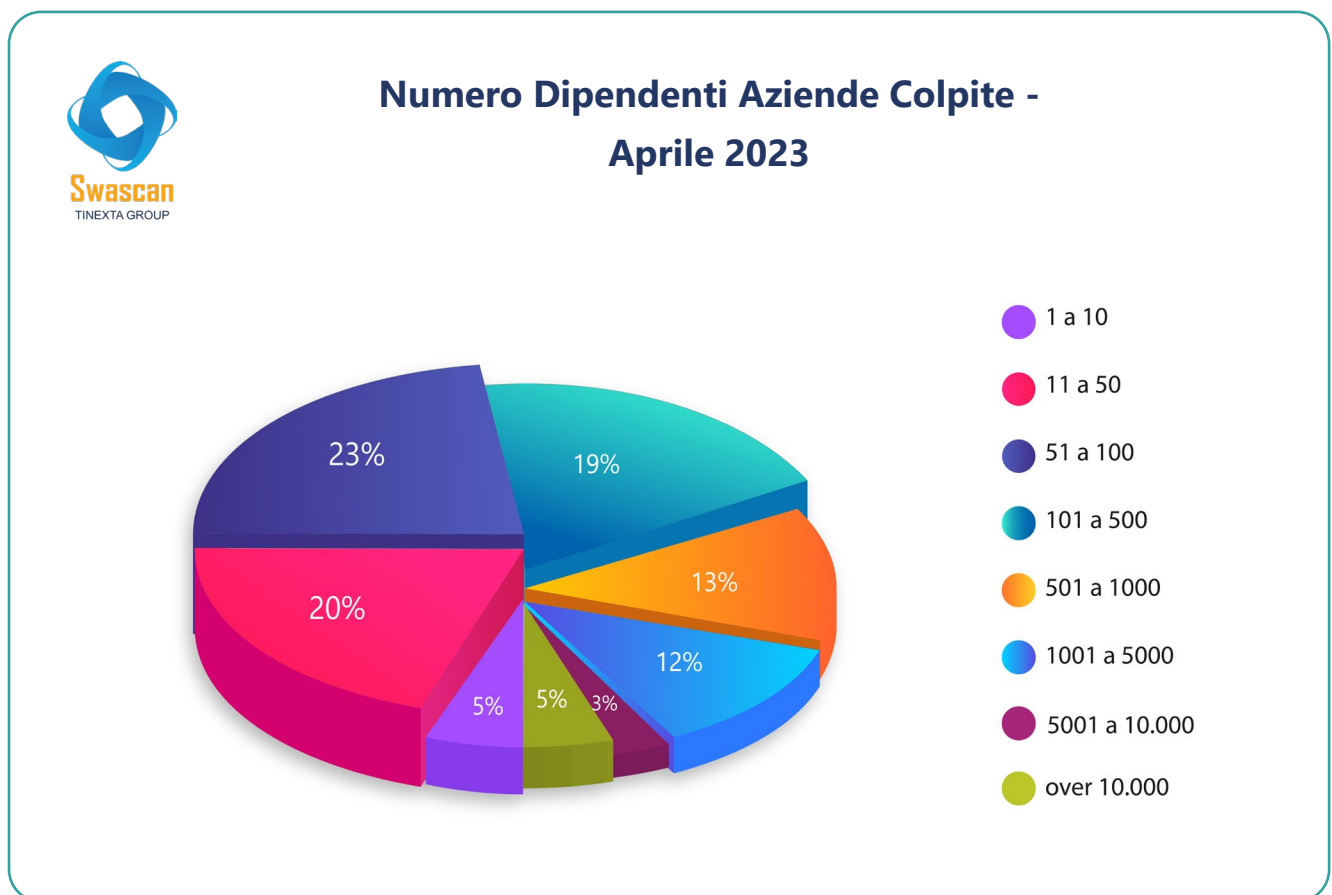
Anche altri settori che hanno subito un numero considerevole di attacchi: questi dati dimostrano che nessun settore è immune dagli attacchi ransomware e sottolineano l'importanza di adottare misure di sicurezza per proteggere i dati aziendali e mitigare gli effetti negativi degli attacchi informatici.

Di seguito riportiamo un'analisi dei settori colpiti nel Q2 2023:



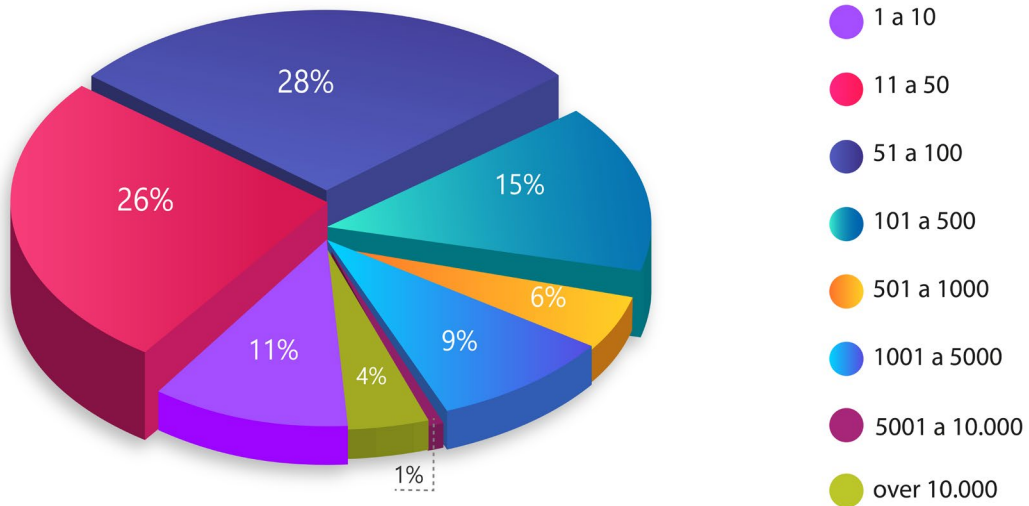
## Cluster vittime in base a personale

Di seguito riportiamo un'analisi del numero di dipendenti delle aziende colpite per ogni mese del Q2 2023, dimostrando come l'attenzione verso la PMI rimanga sempre alta, confermando dunque il trend già analizzato nel Q1 2023:

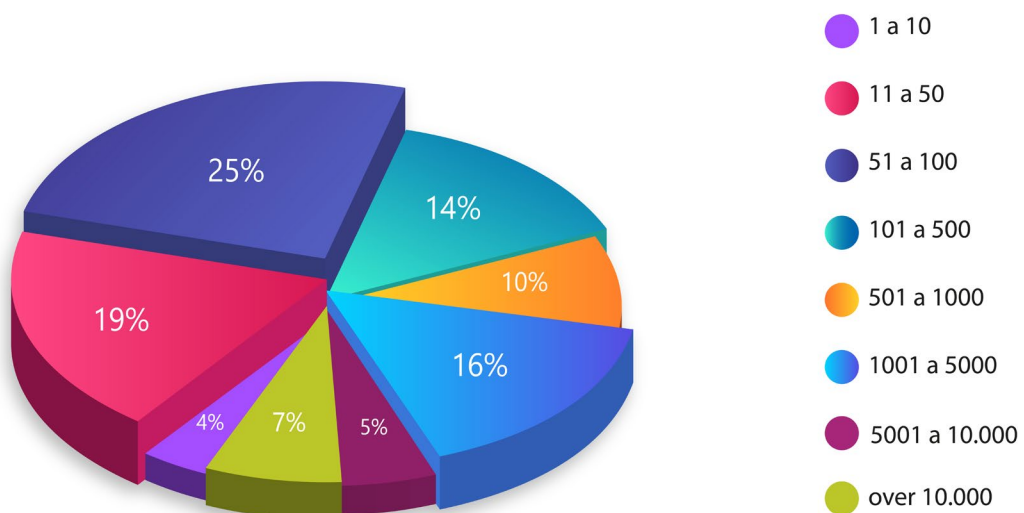




### Numero Dipendenti Aziende Colpite - Maggio 2023



### Numero Dipendenti Aziende Colpite - Giugno 2023



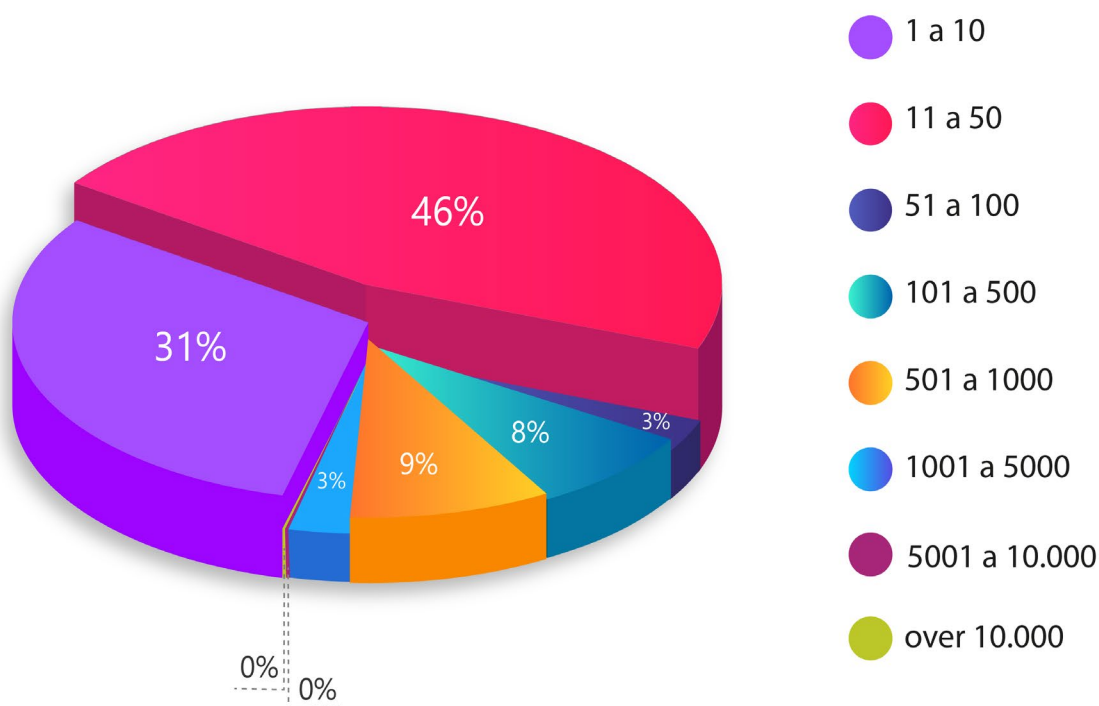
## Cluster vittime in base a personale e fatturato Focus Italia

Nel Q2 2023, gli attacchi ransomware in Italia hanno colpito un totale di 35 aziende: di queste, le piccole e medie imprese con un numero di dipendenti tra 1 e 100 costituiscono la maggioranza delle vittime degli attacchi ransomware, rappresentando l'80% del totale delle aziende colpite. Questo dato indica che i cybercriminali hanno indirizzato i loro attacchi principalmente verso imprese più piccole, considerate più vulnerabili a questo tipo di minaccia a causa di risorse limitate e misure di sicurezza meno sviluppate.

Le aziende con un numero di dipendenti tra 101-500 dipendenti e 501-1000 dipendenti costituiscono l'8% e il 9% rispettivamente. D'altro canto, non sono state riportate vittime tra le aziende più grandi con un numero di dipendenti compreso tra 1001 e 5000, 5001 e 10.000 o oltre 10.000 dipendenti.



**Numero Dipendenti Aziende Colpite -  
Italia - Q2 2023**

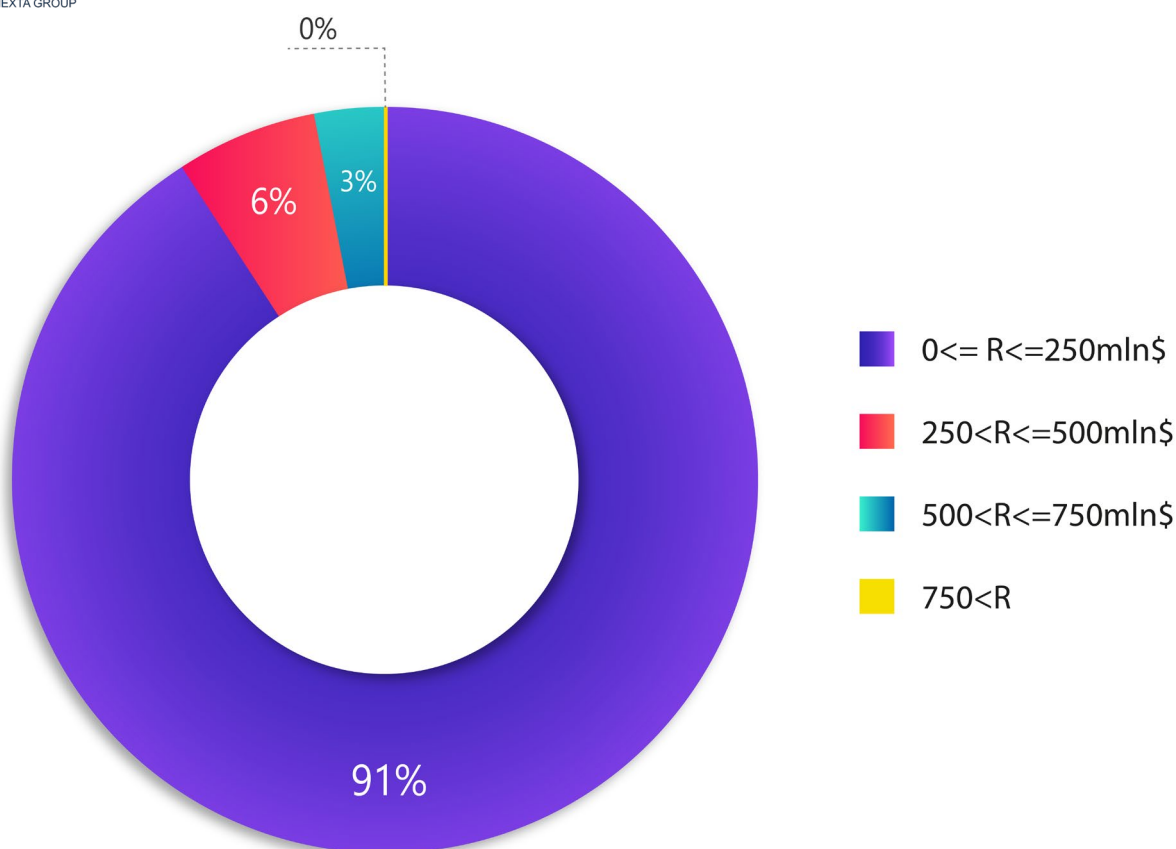




Nel panorama attuale della cybersecurity in Italia, infatti, le piccole e medie imprese (PMI) continuano quotidianamente a subire attacchi ransomware. Le statistiche mostrano chiaramente come le aziende con un fatturato fino a 250 milioni di dollari siano le più colpite, rappresentando una percentuale significativa rispetto ad altre fasce di fatturato. Secondo i dati, il 94% delle aziende colpite da ransomware rientra in questa categoria di fatturato. Questo dato allarmante evidenzia la vulnerabilità delle PMI italiane di fronte a questo tipo di minaccia informatica.



### Spaccato Aziende Colpite In Base A Fatturato- Italia - Q2 2023



Tra i principali attacchi ransomware in Italia nel Q2 2023, diverse aziende italiane sono state prese di mira dalla gang "Lockbit3", subendo attacchi che hanno messo a repentaglio la sicurezza dei dati e dei sistemi aziendali.

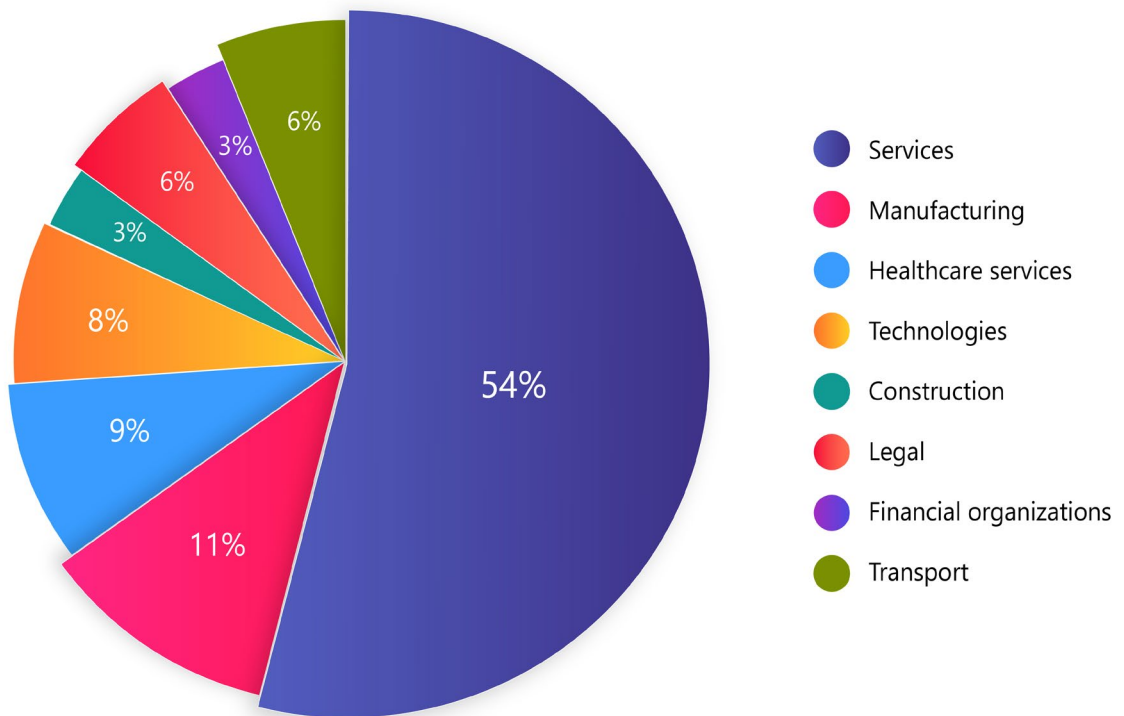
Maggio 2023 ha visto l'Italia scuotersi per una serie di attacchi ransomware che hanno colpito diverse organizzazioni e istituzioni del paese. Questi episodi hanno sollevato gravi preoccupazioni sulla sicurezza informatica e sollecitato la necessità di adottare misure più efficaci per proteggere i dati sensibili.

Tra gli attacchi registrati si riscontra quello ad un noto leader nel settore delle tecnologie dell'informazione in Italia: il loro sistema è stato violato da parte di un gruppo denominato "8base", mettendo a rischio la sicurezza dei loro dati e dei loro clienti. Un'altra organizzazione bersaglio di attacchi durante il mese di maggio, è stata l'ASL 1 - Avezzano Sulmona L'Aquila. Il gruppo criminale Monti ha preso di mira l'organizzazione, mettendo a repentaglio la sicurezza dei dati e creando disagi nel funzionamento dei servizi sanitari.

Questi sono solo alcuni degli attacchi ransomware che hanno colpito le imprese italiane nel Q2 2023, evidenziando come nessun settore è immune dagli attacchi informatici: solo attraverso una solida strategia di sicurezza informatica e la consapevolezza dei rischi associati alle minacce informatiche, le imprese italiane potranno affrontare con successo queste sfide e proteggere la propria attività.

Più nel dettaglio, infatti, le gang ransomware hanno mirato a diversi settori in Italia, con una maggiore attività nel settore dei servizi e nel settore manifatturiero. Questi settori, insieme a quello legale, finanziario, tecnologico e sanitario, rappresentano i principali obiettivi degli attaccanti che cercano di sfruttare le vulnerabilità per ottenere riscatti finanziari.

### Attacchi per settore - Italia - Q2 2023

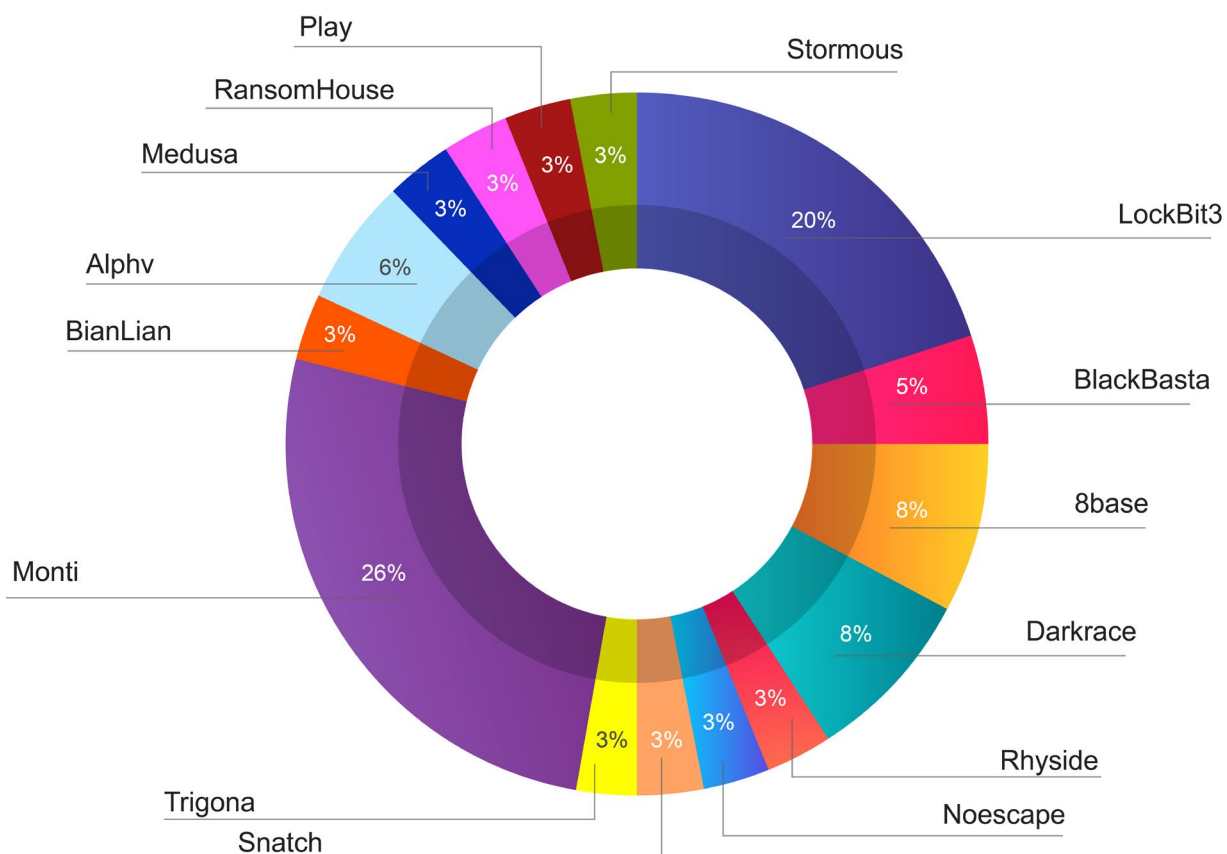


Il settore dei servizi si è dimostrato particolarmente vulnerabile durante il secondo trimestre del 2023, con il 54% degli attacchi in Italia nel periodo considerato: la vasta gamma di aziende e organizzazioni presenti in questo settore offre agli aggressori un ampio campo di azione per cercare di ottenere vantaggi finanziari attraverso estorsioni.

Analizzando le statistiche degli attacchi, inoltre, riportiamo di seguito le gang più attive in Italia e le percentuali di attacchi attribuite a ciascuna di esse.



## Gang più attive - Italia - Q2 2023



Tra tutte le gang ransomware attive in Italia nel secondo trimestre del 2023, **Monti** si è rivelata la più prolifica, rappresentando circa il **26%** di attacchi nel paese, dimostrando un'imponente presenza sul territorio italiano. Anche **Lockbit3** si è confermata come una delle gang ransomware più attive in Italia, con il **20%** degli attacchi.



## CONCLUSIONI

---

Il secondo 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 identificati 43 diversi gruppi di ransomware operanti, con gli Stati Uniti che sono risultati essere la regione più colpita e un totale di 89 paesi che hanno subito attacchi. Tra i gruppi più attivi, spicca Lockbit, che ha causato notevoli danni a molte organizzazioni, raggiungendo un totale di 245 attacchi.

Il quadro generale del Q2 2023 indica un preoccupante aumento del numero di vittime del ransomware rispetto ai trimestri precedenti, con un aumento del 62% rispetto al trimestre precedente, indicando una crescente minaccia per le organizzazioni di tutti i settori e paesi, un aumento del 105% rispetto allo stesso trimestre nello scorso anno, e un aumento del 183% di vittime dall'inizio dell'anno. Concentrando l'attenzione sui dati, emerge come gli Stati Uniti hanno subito il maggior numero di attacchi con 636 aziende vittime. Seguono il Regno Unito con 69 aziende colpite e il Canada con 60. 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 35.

Le PMI continuano ad essere particolarmente vulnerabili a tali attacchi, sia in termini di numero di dipendenti che di fatturato. È preoccupante osservare che gli attacchi ransomware si stanno diffondendo su scala globale, coinvolgendo un totale di 89 paesi in tutto il mondo, dimostrando come gli attacchi ransomware non conoscano confini geografici.

In Europa, tra le gang ransomware più attive nel Q2 2023, LockBit3 si è confermata come la più aggressiva, con 57 attacchi registrati. Seguono PLAY con 30 attacchi, CL0P con 17 attacchi, 8BASE e ALPHV con 16 e 14 attacchi rispettivamente. Queste gang hanno preso di mira diverse industrie, tra cui servizi sanitari, trasporti, tecnologia e servizi finanziari.

Anche in Europa i dati relativi al Q2 2023 dimostrano come le PMI con un numero ridotto di dipendenti, comprese tra 1 e 50, siano le più colpite, rappresentando l'87% delle vittime segnalate.

Risulta allarmante che gli attacchi ransomware stiano colpendo aziende di diverse industrie e settori. In Italia, le aziende del settore dei servizi sono state le più colpite, rappresentando il 54% degli attacchi nel periodo considerato. Tuttavia, è importante sottolineare che nessun settore è al sicuro da questa minaccia digitale in rapida evoluzione: le aziende di settori come il manifatturiero, i servizi finanziari, la sanità e il trasporto sono state tutte prese di mira dagli attacchi ransomware.

La minaccia delle credenziali di accesso in vendita rappresenta ad oggi una preoccupazione sia per le aziende sia per i consumatori in tutto il mondo. Secondo i dati raccolti in questo Q2 sono difatti emersi

7'756'466 dispositivi compromessi dai quali sono stati esfiltrate credenziali di accesso a portali interni e/o pubblici, informazioni personali, wallet di cryptovalute ed accessi ad online banking che possono essere acquistati illegalmente sui mercati nel Deep e Dark Web. L'Europa ricopre il 17,7% dei dispositivi totali mentre l'Italia ricopre il 2,4% del totale e il 13,8% rispetto l'Europa. La facilità di reperire queste credenziali presenta quindi un rischio elevato di accesso non autorizzato a sistemi informatici che potrebbe portare ad attacchi più invasivi quali ad esempio un attacco Ransomware.

Il rischio tecnologico derivato da vulnerabilità inoltre rimane uno dei principali vettori di attacco iniziale da parte dei Threat Actor. Nel Q2 sono state rilevate un totale di 7'514 vulnerabilità su prodotti tecnologici con un focus su quelle che ad oggi vengono maggiormente sfruttate e discusse da gang Ransomware. Una fra tutte è la CVE-2023-34362 che ha concesso alla gang C10p di compromettere più di 150 organizzazioni tramite lo sfruttamento della stessa.

La minaccia del malware continua a rappresentare una preoccupazione per le aziende e i consumatori in tutto il mondo. Secondo gli ultimi dati, il malware più diffuso risulta essere Mirai con il 53,4%, botnet largamente impiegata in attacchi di DDoS, seguono poi Hajime con il 21,1% e Qakbot con il 10,8%.

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.

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.

Nel Q2 sono inoltre state analizzate i maggiori Framework di Command&Control che vengono utilizzati attivamente dai Threat Actor durante gli attacchi. In merito alla classifica delle C2 rilevate è emerso come CobalStrike sia il più diffuso, occupando il primo posto con il 55,24%, mentre al secondo e terzo posto sono presenti Metasploit e Silver con rispettivamente 28,33% e 12,47%.

Rimane quindi fondamentale avvalersi di soluzioni di Threat Intelligence per identificare queste minacce proattivamente e un servizio di monitoraggio capace di mitigare prontamente queste minacce.

Il phishing, infine, continua ad essere tra i primi vettori di attacco: la campagna maggiormente osservata risulta Office365, utilizzata dagli attaccanti circa 25 volte ogni 100 campagne, seguita da Facebook e DHL Airways usate rispettivamente al 21% e al 9%.

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 Business Email Compromise (BEC) la facciano ancora da padrone.

## L'opinione del CEO di Swascan Pierguido Iezzi

---

L'incremento nei casi di attacchi di phishing e ransomware ha raggiunto proporzioni che non sembrano spiegabili completamente come fenomeni casuali. Queste offensive, oltre ad essere orchestrate molto sovente da individui o gruppi con un certo livello di competenza tecnica e specifiche motivazioni, seguono da anni una curva di crescita insolitamente elevata. Questo aumento potrebbe quindi indicare in parte l'attuazione di una strategia calcolata da parte di coloro che stanno dietro agli attacchi.

D'altra parte, il trend non solo sta causando danni significativi alle economie dei Paesi colpiti, inclusa l'Italia, ma sta anche mettendo in discussione la percezione di sicurezza sia tra le persone comuni sia tra le organizzazioni. Non possiamo sottovalutare il fatto che questi attacchi di phishing e ransomware, sempre più frequenti, possano influenzare l'opinione pubblica sulla capacità dei governi di proteggere i cittadini e le risorse nazionali.

Infatti, da tempo, il cyber crime è stato incluso tra gli strumenti della cognitive war; in cui l'obiettivo non si limita solo all'accesso o al controllo dei sistemi, ma comprende anche l'influenza sulla percezione pubblica, la destabilizzazione e la manipolazione dell'opinione generale.

Come se non bastasse, l'aumento di attacchi di phishing e ransomware potrebbe anche incrementare la richiesta di assistenza verso il governo da parte delle vittime di queste offensive digitali, andando quindi a impattare in maniera sostanziale budget e risorse a disposizione della PA.

La sfida posta dalle minacce cibernetiche contemporanee trascende la semplice capacità di risposta. L'ambiente digitale, sempre in evoluzione, ha completamente trasformato il campo di battaglia, rendendo obsoleti molti approcci tradizionali alla sicurezza. Sebbene la collaborazione e la consapevolezza siano componenti fondamentali, ciò che è davvero necessario è una radicale riformulazione della nostra strategia di difesa nazionale. Significa non solo adottare tecnologie all'avanguardia e riconsiderare le priorità di finanziamento, ma anche mettere in atto meccanismi di presidio e monitoraggio della rete.

La rete, infatti, è diventata il tessuto connettivo della nostra società, essenziale per la tutela degli interessi nazionali. Il controllo di questo dominio digitale è cruciale non solo per proteggere infrastrutture e dati, ma anche per salvaguardare il prestigio del "Made in Italy" e, ancor di più, per proteggere i cittadini da minacce dirette e indirette. In un'epoca in cui le informazioni si muovono a velocità inimmaginabili e in cui l'influenza digitale può avere ripercussioni reali sulle vite delle persone, garantire la sicurezza della rete non è più un'opzione ma una necessità imperativa.

Le partnership con il settore privato e le istituzioni accademiche sono fondamentali in questo contesto, ma la vera rivoluzione deve avvenire a livello istituzionale. Le agenzie governative devono evolvere, collaborando in modo più stretto e riqualificandosi continuamente, poiché la natura mutevole delle minacce cibernetiche richiede un nuovo paradigma di pensiero e azione.

L'emergere di nuovi domini nel cyber warfare sottolinea ulteriormente l'importanza di questa evoluzione. Dai concetti di Multi-domain warfare e Algorithmic warfare, che vedono l'integrazione di vari domini di combattimento e l'importanza crescente dell'intelligenza artificiale, all'allarmante Tech-enabled information warfare, il panorama della difesa è in continua evoluzione.

Termini come Hyper war e Automated warfare ci mostrano una realtà in cui la rapidità e l'automazione dominano il campo di battaglia. E nel mezzo di queste strategie avanzate, le Cyber-kinetic operations illustrano la convergenza del mondo digitale con quello fisico.

In conclusione, nell'era digitale, una strategia di difesa preventiva (analisi del rischio) e di Incident Management non è più sostenibile. Ciò che è necessario ora è un approccio predittivo e proattivo, un impegno profondo verso l'innovazione, e la capacità di rivedere e adattare le strategie di difesa alla luce delle continue minacce emergenti. Presidiare e monitorare la rete, proteggendo così il patrimonio, l'economia e i cittadini, è diventato un pilastro fondamentale di questa nuova era della difesa nazionale.



# COME DIFENDERSI DAL RANSOMWARE: IL CYBER SECURITY FRAMEWORK

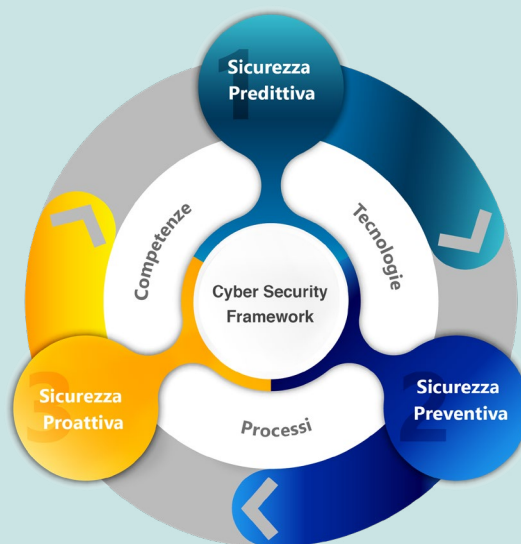
L'approccio migliore per aumentare la resilienza del perimetro passa per i tre pilastri della Cyber Security moderna. Per questo motivo vanno consolidati e rispettati i tre canoni di:

- **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

## Action Plan

---

In linea con le best practice descritte nel cyber security framework è consigliato implementare un action plan di cyber security basato sui seguenti step:

### 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 dispositivi di clienti, fornitori e dipendenti
- Botnet con credenziali e relative url di login page
- Typosquatting/Phishing
- Surface
- Top Manager Analysis

## Sicurezza Preventiva:

**Vulnerability Assessment:** Eseguo 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.

**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. Quest'ultimi, infatti, grazie a tali 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 (Cyber Academy):** 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.

## Sicurezza Proattiva:



**SOC:** 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 nell'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 Team:** Il Cyber Incident Response Team by Swascan è un servizio di Pronto Intervento Cyber h24 con obiettivo e scopo di supportare le aziende nell'attività di risposta e gestione degli incidenti di sicurezza informatica e attacchi Ransomware.

In linea con lo standard internazionale NIST SP 800-61rev2 Computer Security Incident Handling Guide, a seguito di un incidente informatico l'IRT di Swascan ha l'obiettivo di:

- Contenimento dei possibili danni
- Determinare i possibili danni e impatti
- Garantire una risposta efficace ed efficiente
- Supportare il ripristino della Business Continuity
- Fornire indicazioni e suggerimenti per prevenire il verificarsi di incidenti futuri



## 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:**

Riccardo Michetti  
Riccardo D'Ambrosio  
Martina Fonzo

## **Technical Contributors:**

Soc Team Swascan

## **Editing & Graphics:**

Federico Giberti  
Melissa Keysomi

## **Contact Info**

Milano  
+39 0278620700  
[www.swascan.com](http://www.swascan.com)  
[info@swascan.com](mailto:info@swascan.com)  
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI