Rapporto Cyber 1° Semestre 2023

Curato dall'Assintel Cyber Think Tank

CYBER Think Tank ASSINTEL

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

Swascan
TINEXTA GROUP

mediatech

HACKMANAC

Sommario

H1 2023

Il primo semestre 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, malware e phishing, fornendo un quadro dettagliato delle minacce emergenti e delle tendenze in evoluzione.

Durante l'H1 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, soprattutto 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. 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, 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.

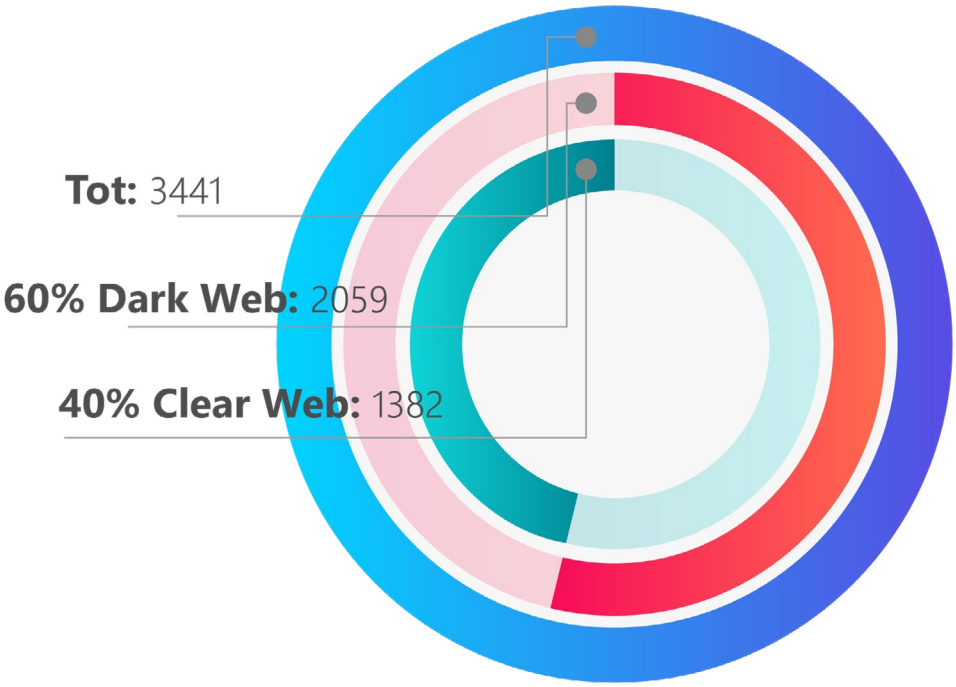
I CYBER ATTACCHI NEL PRIMO SEMESTRE 2023

Analizzando i cyber attacchi andati a buon fine e divenuti di pubblico dominio, ogni anno abbiamo visto un aumento significativo rispetto al periodo precedente.

A partire da gennaio 2023 però abbiamo incluso nel nostro campione anche attacchi collezionati dal Dark Web e il risultato è stato notevole.

Su **3.441 incidenti** totali analizzati nel primo semestre dell'anno, un numero già impressionante considerando che supera di gran lunga il totale dell'anno precedente, **2.059, ovvero il 60%,** provengono esclusivamente da fonti del **Dark Web**.

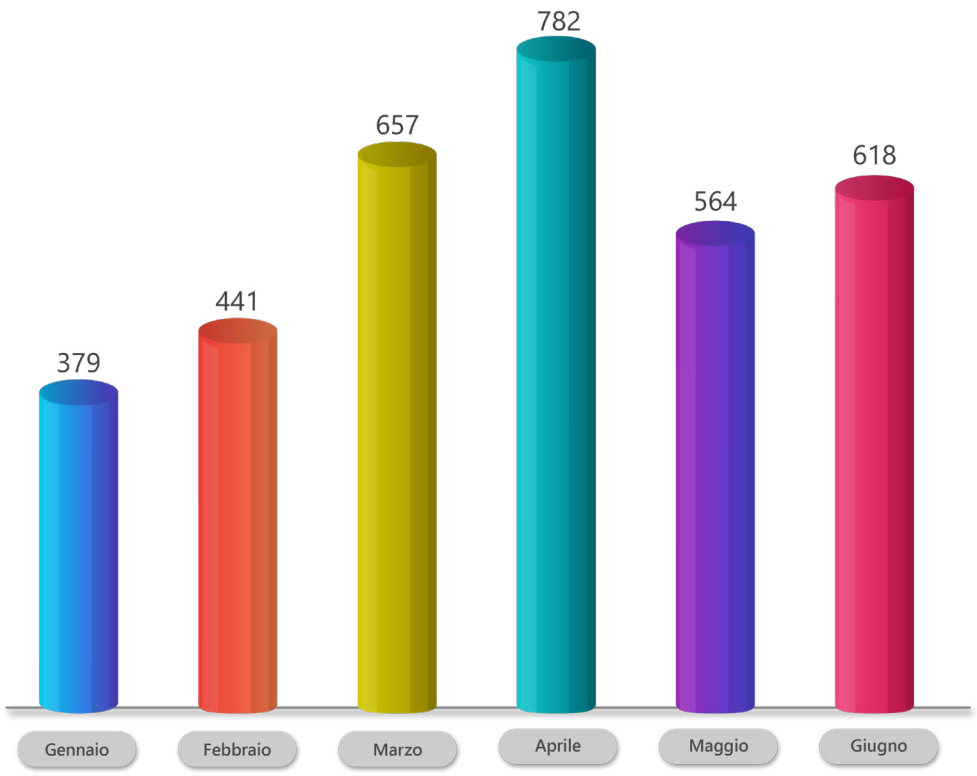
Distribuzione delle fonti dei cyber attacchi H1 2023



© Hackmanac Global Cyber Attacks Report 2023

Anche le medie mensili sono aumentate considerevolmente e nel primo semestre arrivano a **574** (384 solo per quanto riguarda gli incidenti collezionati dal Dark Web).

Cyber attacchi per mese nel primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

Come sempre abbiamo notato un picco di cyber attacchi in primavera: nel primo semestre 2023 aprile è il mese con il numero maggiore di attacchi, **782 in totale**.

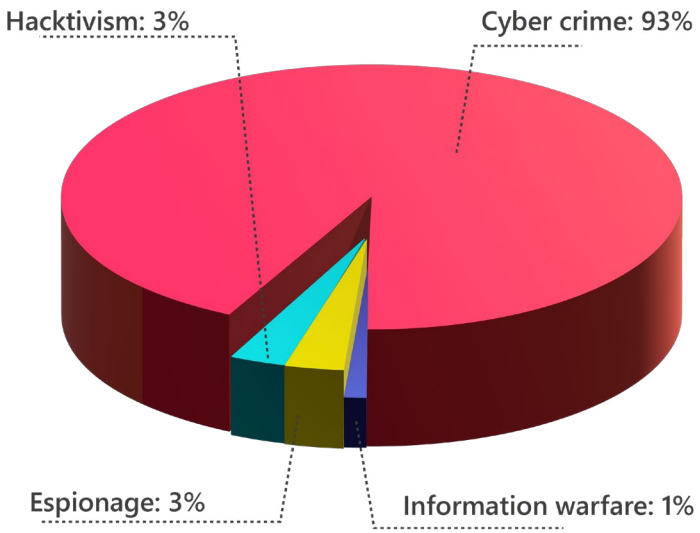
A seguire marzo (**657**) e giugno (**618**).

Gennaio e febbraio sono invece i mesi in cui abbiamo riscontrato meno attività criminali (rispettivamente **379** e **441** cyber attacchi).

Gli attaccanti

Il **Cybercrime** è da anni la principale minaccia, considerando anche che, tra gli attacchi di pubblico dominio alcune categorie come **Espionage** e **Information Warfare** sono sotto rappresentate rispetto al reale numero di incidenti che avvengono in questi ambiti.

Distribuzione attaccanti primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

Nel 2023 il fenomeno del cybercrime, che negli anni precedenti è cresciuto in maniera continua, raggiunge il **93%** degli attacchi totali del primo semestre, a discapito dei fenomeni di **Espionage / Sabotage** e **Information Warfare** (rispettivamente **3%** e **1%**), in notevole discesa rispetto all'anno precedente.

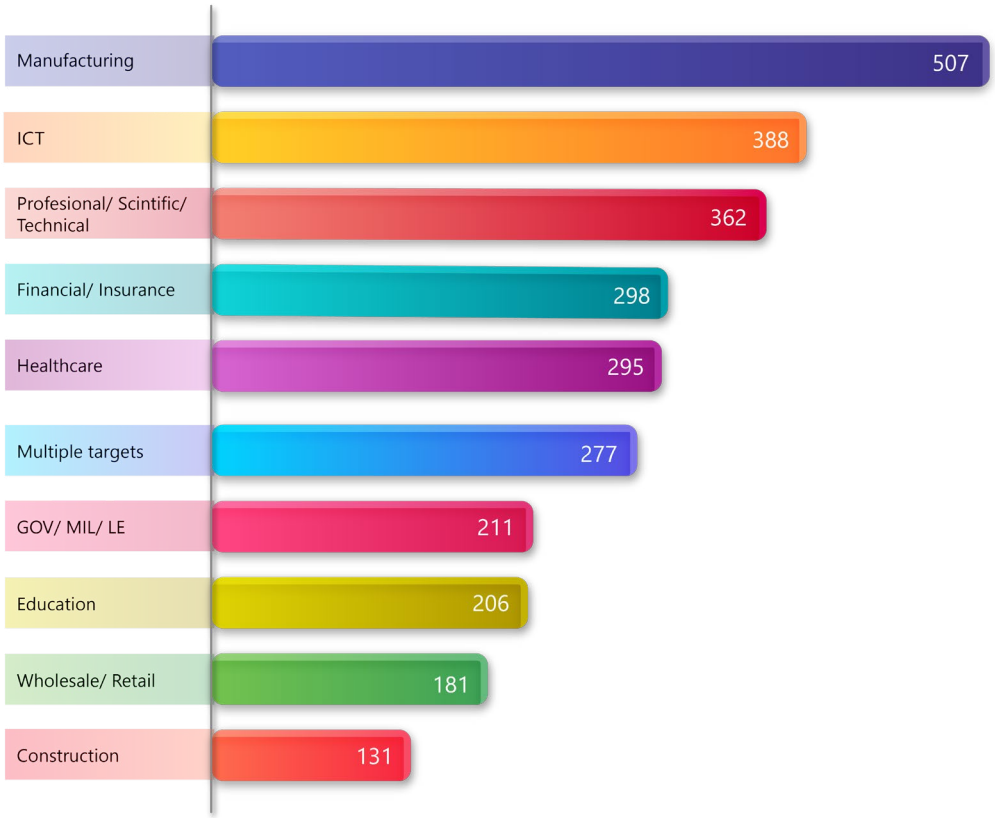
Resta costante invece il ricorso all'**Hacktivism** (**3%** del totale).

Le vittime

Andando ad analizzare le vittime principali dei cyber attacchi del primo semestre 2023, l'ambito **Manufacturing** è in assoluto il più preso di mira arrivando al **15%** del totale degli attacchi.

Questa è una novità rispetto agli anni precedenti dove Multiple Targets era la categoria con il più alto numero di incidenti.

Distribuzione delle prime 10 vittime nel primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

Nel 2023 la categoria Multiple targets viene presa di mira solo nell'8% dei casi e per la prima volta figura solo al sesto posto tra le prime 10 vittime del semestre

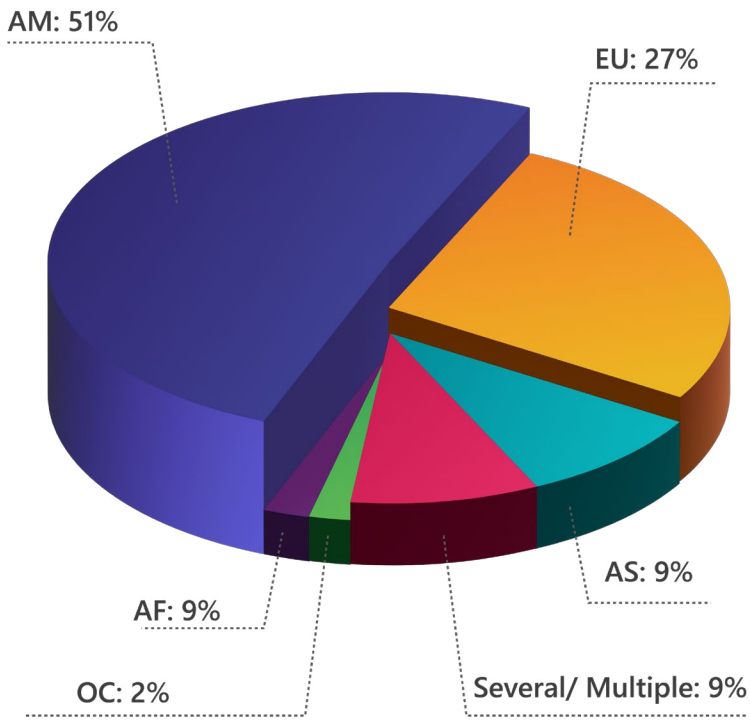
Al secondo posto tra i settori maggiormente presi di mira figura l'ambito **ICT** (11% del totale) a parimerito con **Professional / Scientific / Technical** (11%), dove invece gli attacchi sono cresciuti considerevolmente.

A seguire **Financial / Insurance** ed **Healthcare** (entrambi 9% del totale).

La geografia delle vittime

Nel primo semestre 2023 tornano a crescere le vittime sul territorio americano che salgono al **51%** dopo la flessione degli anni precedenti.

Distribuzione delle vittime per continente nel primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

La crescita degli attacchi americani non avviene però a discapito di quelli verso l'**Europa** che nel 2023 arrivano al **27%** del totale.

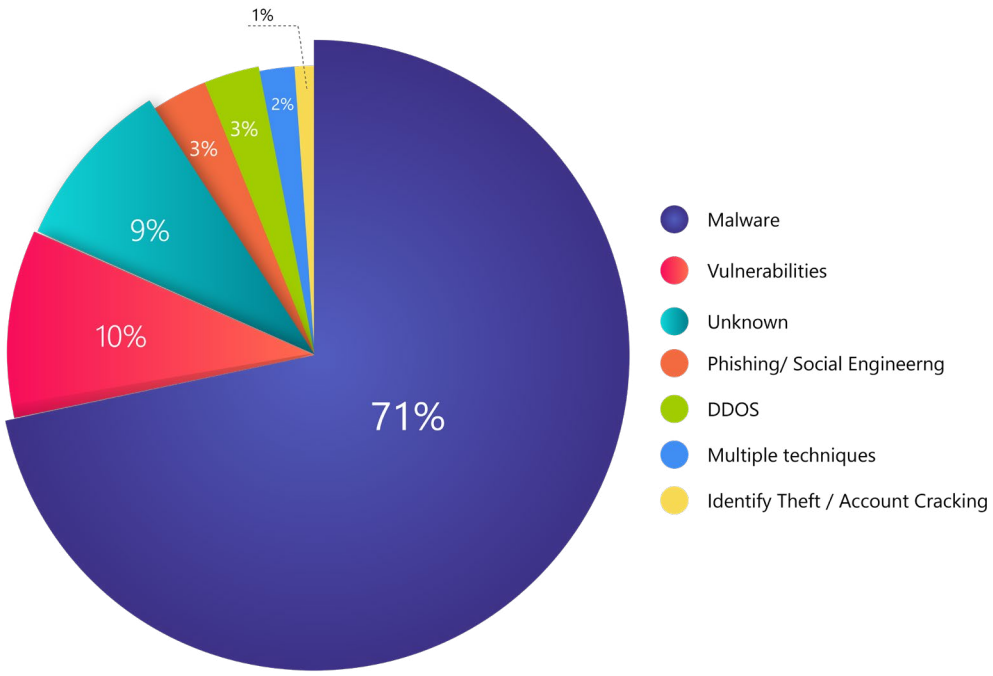
Scendono invece considerevolmente gli attacchi verso località multiple (9% del totale), a riprova del fatto che una caratteristica dell'anno in corso è che gli attacchi sono più mirati.

Restano sostanzialmente invariate, o variano di poco, le quote di Asia (9%), Oceania (2%), mentre raddoppiano invece gli attacchi verso il territorio africano giunti al 2% degli incidenti totali.

Le tecniche di attacco

Non è un segreto che da diversi anni il Malware spicca tra le tecniche di attacco più utilizzate, anche grazie alla notevole resa dei ransomware per i cyber criminali.

Distribuzione delle tecniche di attacco nel primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

Ma nel 2023 il ricorso a questa tecnica aumenta pericolosamente, arrivando quasi a raddoppiare e toccando il **71%** del totale degli attacchi.

Seguono lo sfruttamento delle **vulnerabilità (10%)**, in leggero calo rispetto all'anno scorso, e le tecniche sconosciute (9%), in netta diminuzione, un ulteriore segnale che gli attacchi nel 2023 prediligono tecniche più affidabili e consolidate.

Diminuisce inoltre il ricorso a Phishing / Social Engineering (3%), DDoS (3%), tecniche multiple (2%), Identity Theft / Account Cracking (1%).

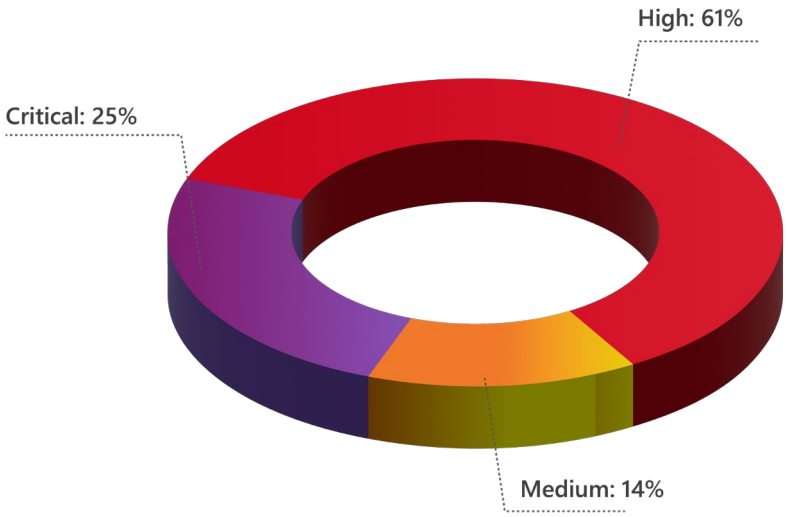
I Web attack, che negli anni precedenti rappresentavano una minima parte degli attacchi totali, raggiungono quota 0 durante i primi mesi dell'anno.

Gli impatti

La valutazione degli impatti dei cyber attacchi è fondamentale per comprendere quanto questi siano stati incisivi e tiene in considerazione variabili geopolitiche, economiche, tecnologiche e di reputazione.

Per riconoscere i diversi gradi di gravità degli attacchi abbiamo individuato 4 classi di severity: **Low**, **Medium**, **High** e **Critical**.

Distribuzione delle severity degli attacchi nel primo semestre 2023



© Hackmanac Global Cyber Attacks Report 2023

Nel primo semestre dell'anno in corso gli attacchi con impatti gravi o gravissimi sono l'**86%** del totale.

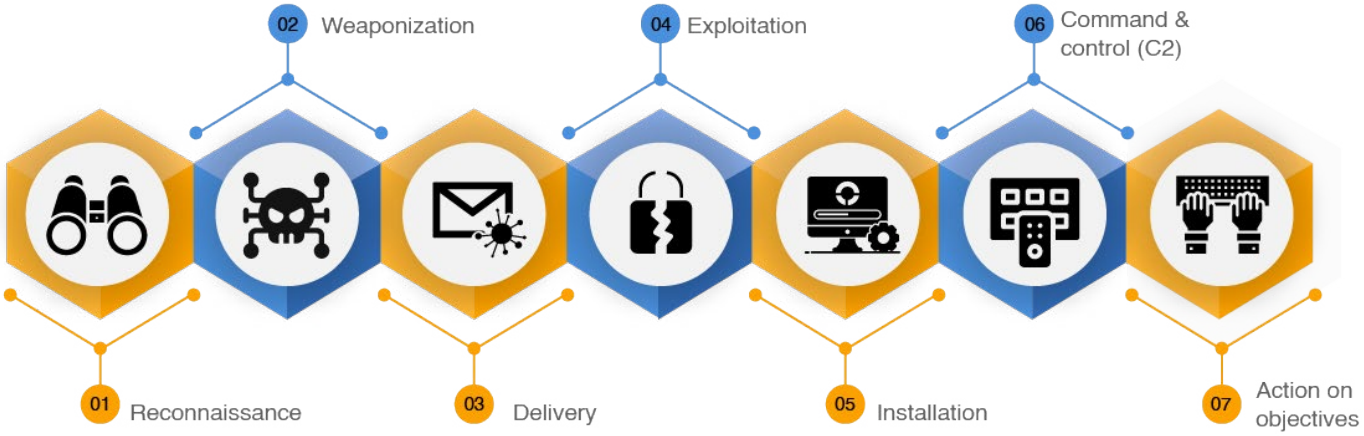
Ma l'aspetto più problematico è che un quarto degli attacchi (**25%**) hanno avuto impatti **critici**, una quota impressionante considerando che le ripercussioni si possono quantificare in termini economici, legali o reputazionali.

Crescono complessivamente gli attacchi con impatti gravi (High **61%** del totale degli attacchi), mentre diminuiscono complessivamente quelli con impatti medi (**14%**).

Gli impatti bassi restano allo 0%.

LA CYBER KILL CHAIN: un approccio strategico per difendersi dagli attacchi informatici

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.



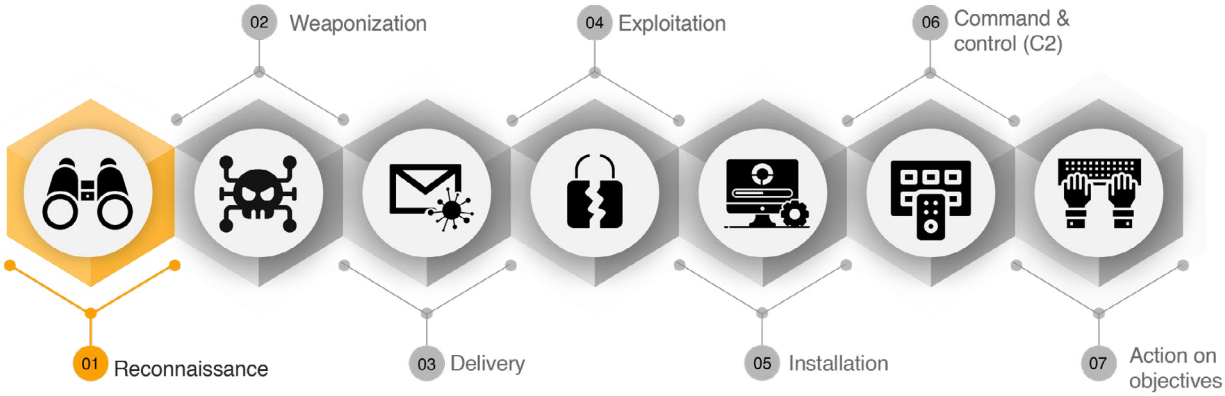
Le sette fasi della Cyber Kill Chain sono le seguenti:

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

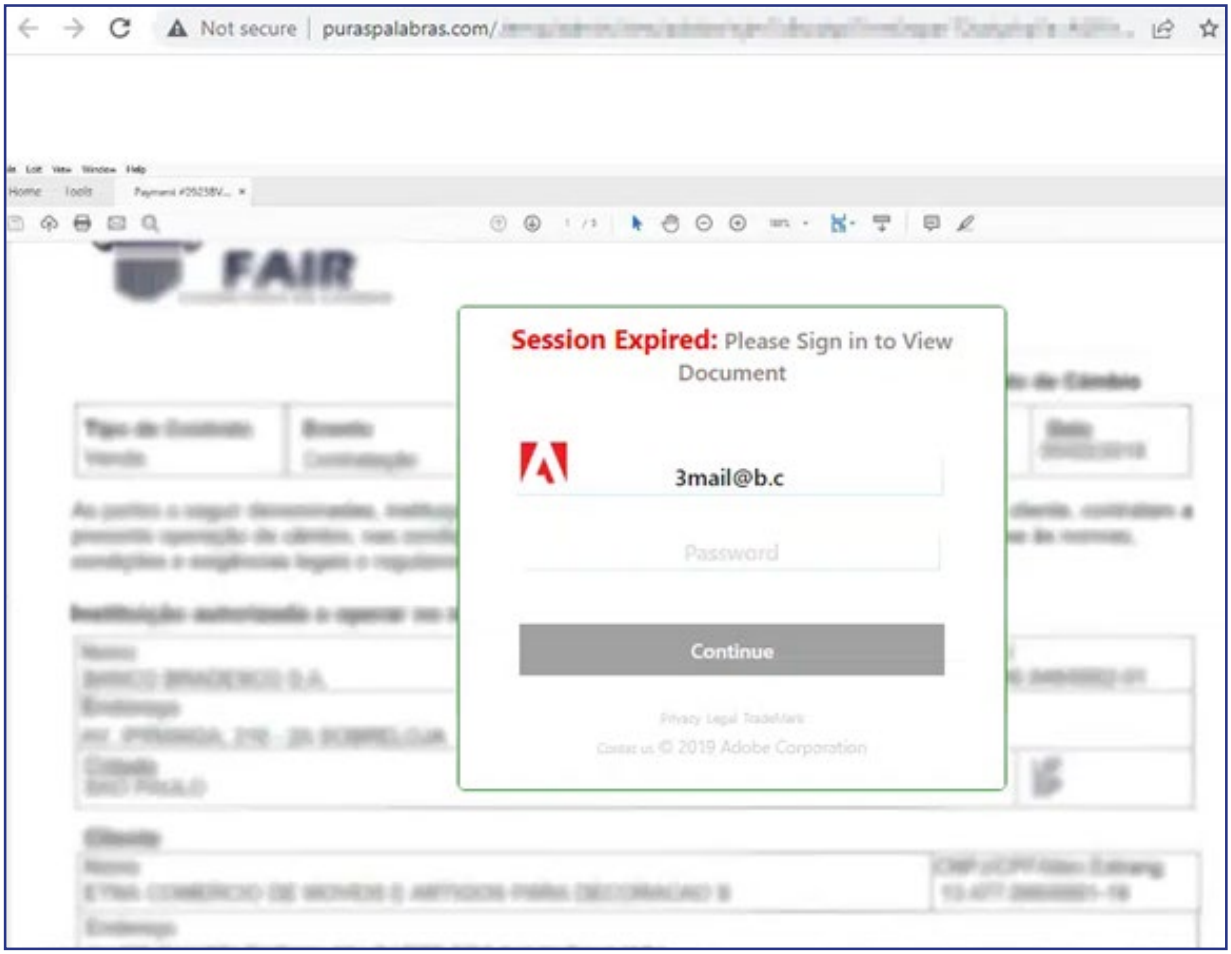


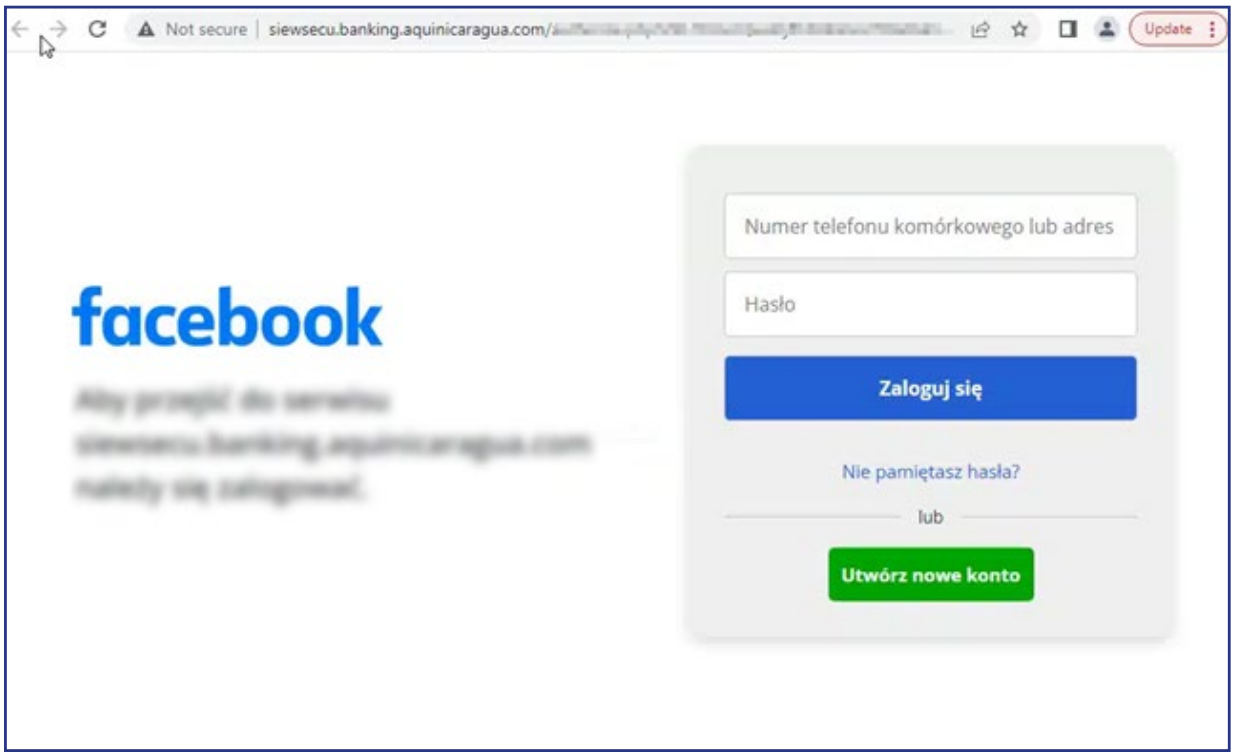
La fase di reconnaissance è la prima importante tappa all'interno della Cyber Kill Chain, durante la quale gli attaccanti raccolgono informazioni preziose per pianificare un attacco mirato. Durante questa fase, vengono adottate diverse strategie, tra cui, ad esempio, la raccolta di credenziali da mercati 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.

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. Per esempio, 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:


Not secure | puraspalabras.com/
FAIR
Session Expired: Please Sign in to View Document
3mail@b.c
Password
Continue
Privacy Legal Trademarks
Contact us © 2019 Adobe Corporation

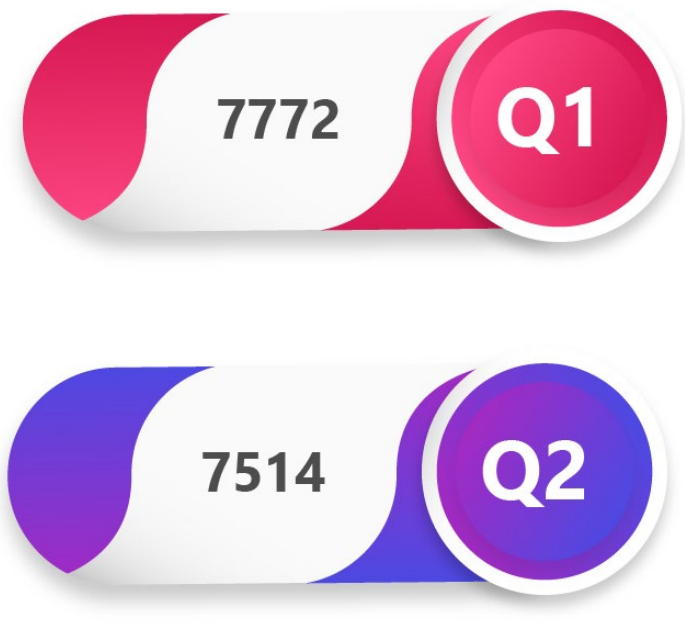

Not secure | siewsecu.banking.aquinicaragua.com/
Update
facebook
Numer telefonu komórkowego lub adres
Hasło
Zaloguj się
Nie pamiętasz hasła?
lub
Utwórz nowe konto

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.

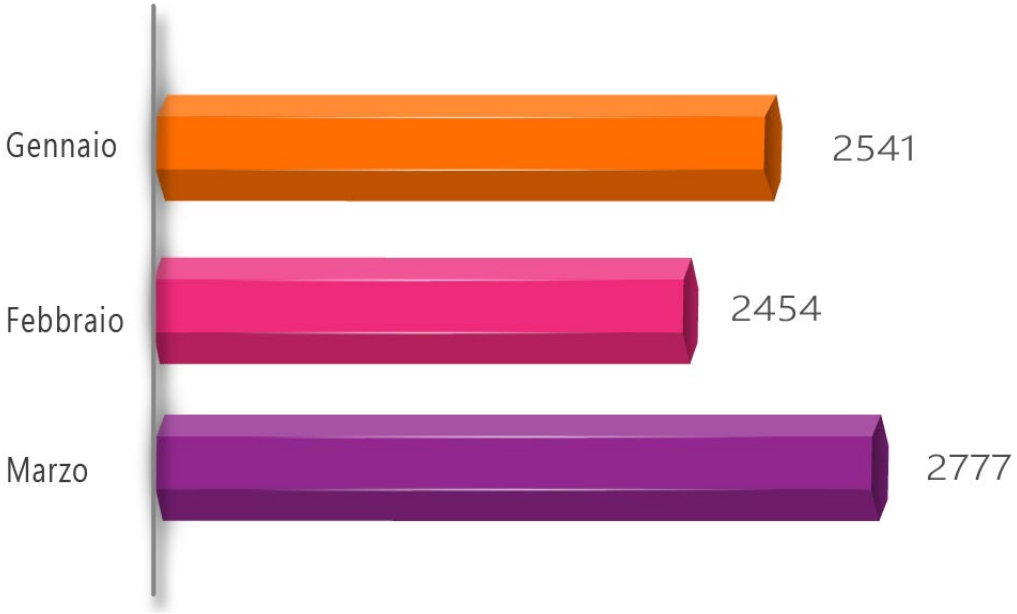
Nel Q1 relativo al 2023 erano state pubblicate 7'772 nuove CVE contro le 7'514 pubblicate nel Q2:

CVE
Q1 vs Q2 2023

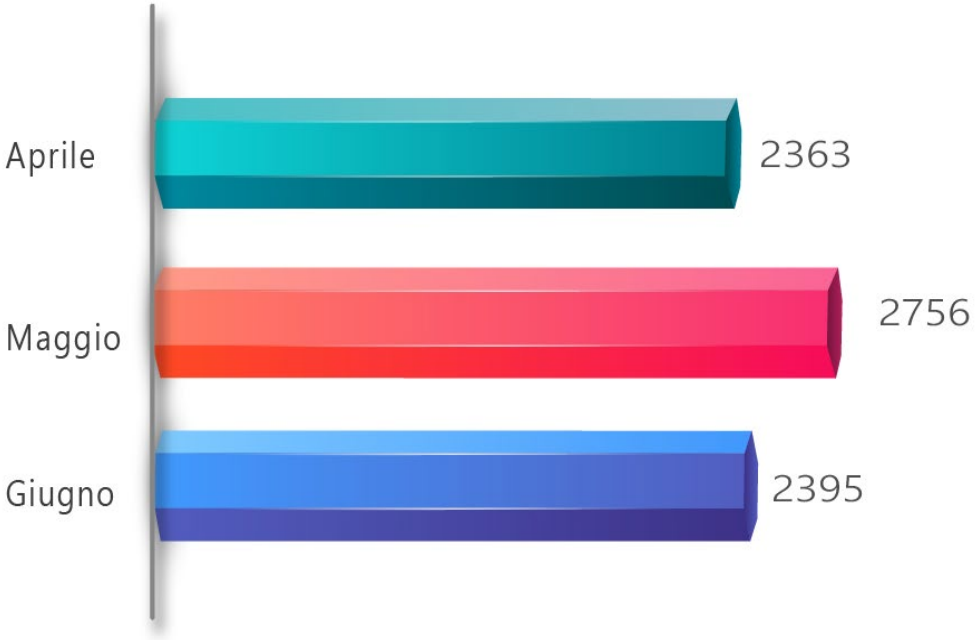


CVE - tracciate e segnalate dalla MITRE Corporation. Questo numero fa riferimento alle nuove vulnerabilità riconosciute e segnalate nel periodo in oggetto

CVE- Q1 2023



CVE- Q2 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, infostealer 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. Possono infatti 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.

DELIVERY

Una delle minacce più diffuse e dannose rilevate nell'H1 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: i trend

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.

Il Q1 2023 è stato caratterizzato da una crescente minaccia degli attacchi di spearphishing, Business Email Compromise (BEC) e Email 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, i quali sfruttano metodi come il typosquatting o lo spoofing di domini aziendali nelle intestazioni delle e-mail.

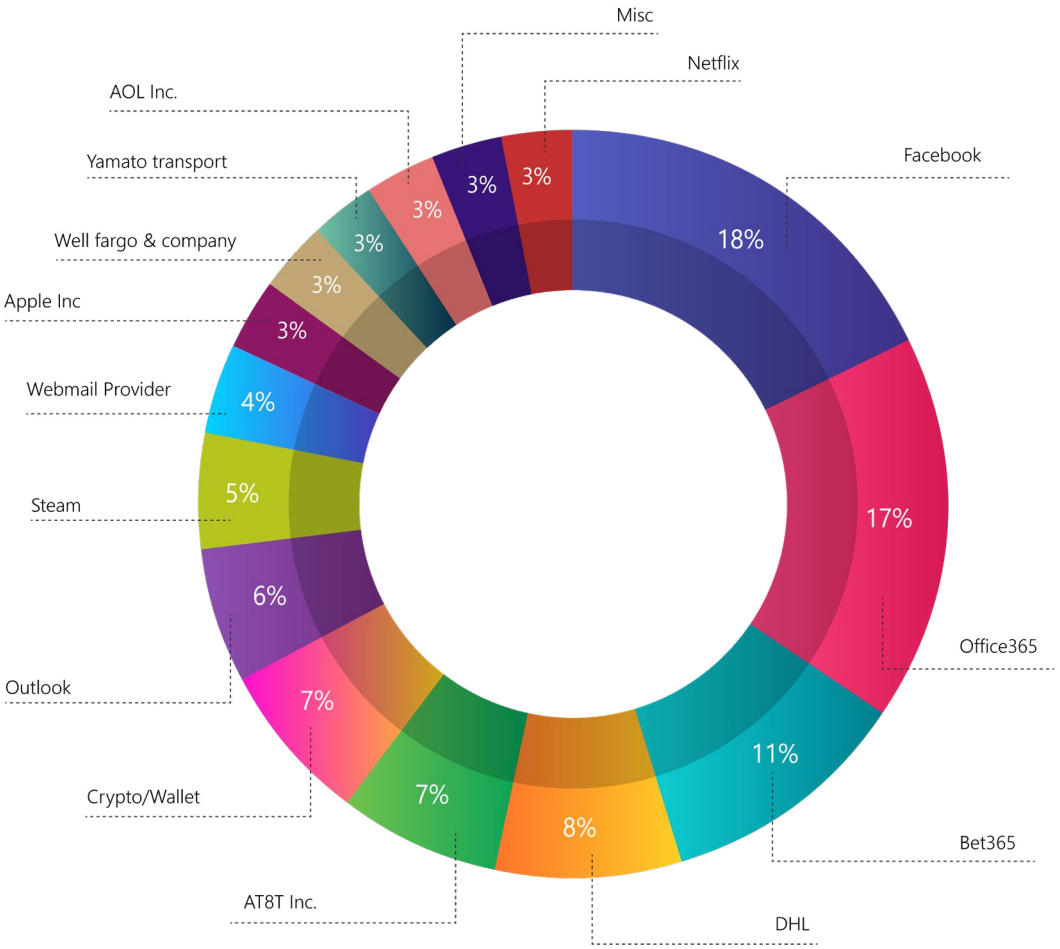
Il phishing è una tecnica utilizzata dagli hacker per rubare informazioni personali e finanziarie dalle vittime, che vengono ingannate attraverso e-mail, siti web o messaggi che sembrano legittimi. Nel Q1 2023, diverse aziende e servizi online sono stati bersaglio di campagne di phishing, con **Facebook** 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 troviamo **Office365** con il **17%** degli attacchi di phishing, seguito dal sito web di scommesse **Bet365** con l'**11%**. Quest'ultimo è stato spesso utilizzato come esca per convincere gli utenti ad inserire le loro informazioni di pagamento.

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

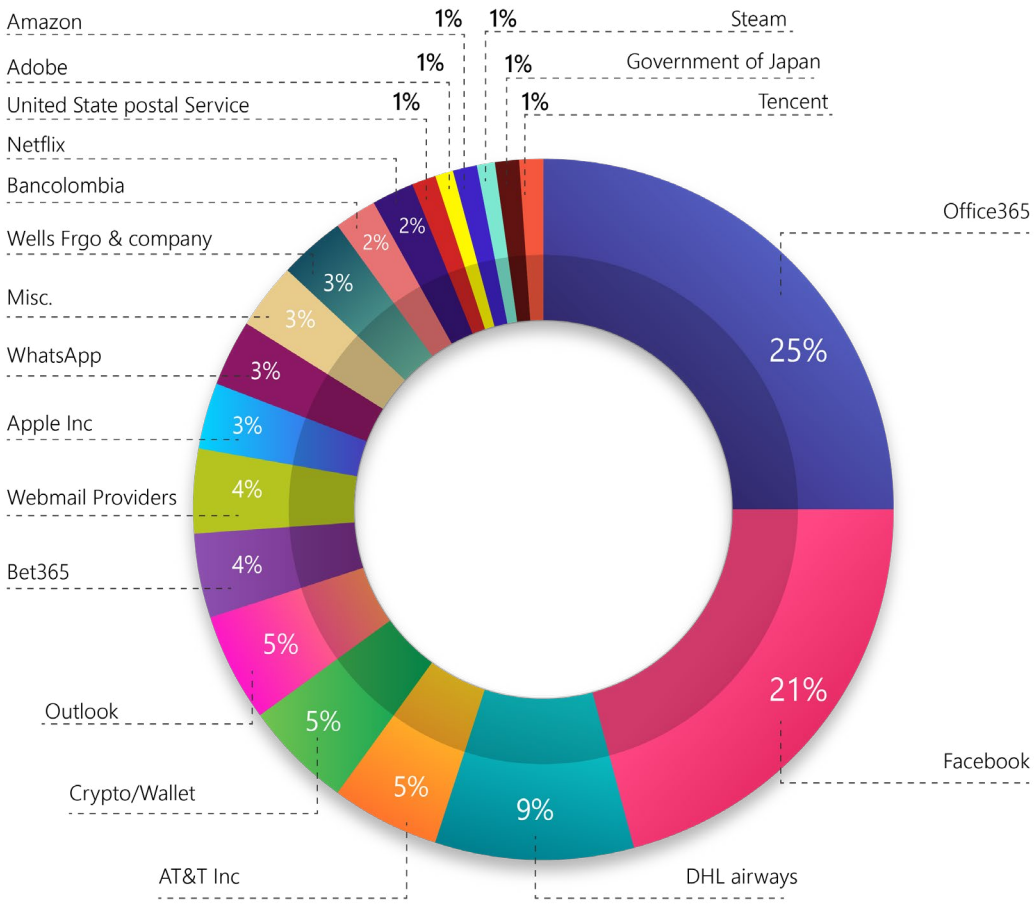
Il resto della lista include AT&T Inc. (7%), Crypto/Wallet (7%), Outlook (6%), Steam (5%), Webmail Providers (4%), Apple Inc. (3%), Wells Fargo & Company (3%), Yamato Transport (3%), AOL Inc. (3%), Netflix Inc. (3%) e Credit Agricole S.A. (3%).

Phishing campaign - Q1 2023



Nel Q2 tra i brand più imitati troviamo: **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.

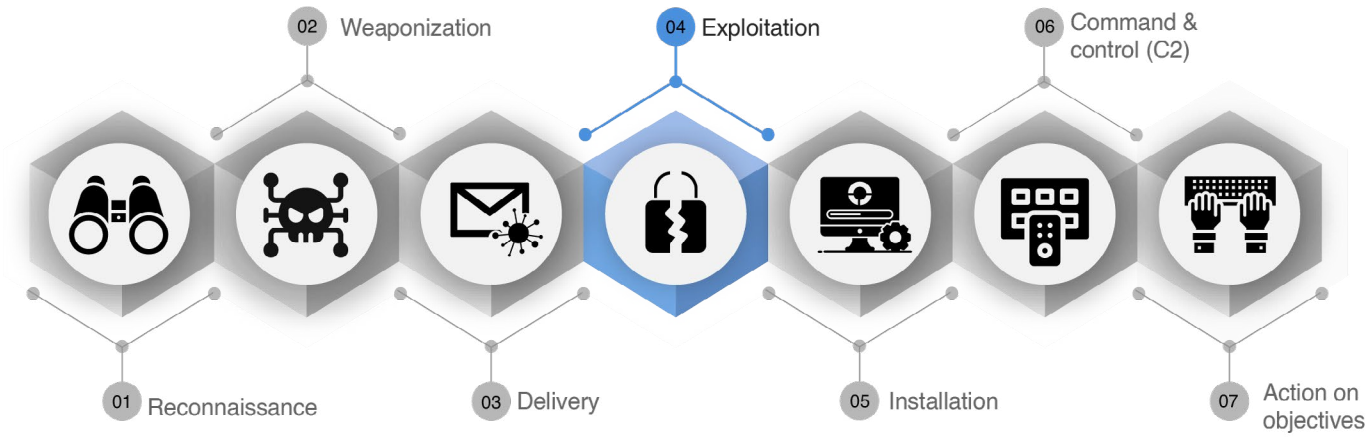
Phishing campaign - Q2 2023



Al terzo posto DHL con il 9%, spesso sfruttato dagli hacker per creare e-mail contraffatte che sembrino 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%), Credit Agricole S.A. (3%), Bancolombia (2%), Netflix (2%), United States Postal Service (1%) Adobe Inc. (1%) Amazon (1%), Steam (1%), Government of Japan (1%) e Tencent (1%).

EXPLOITATION



Nel primo semestre 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:

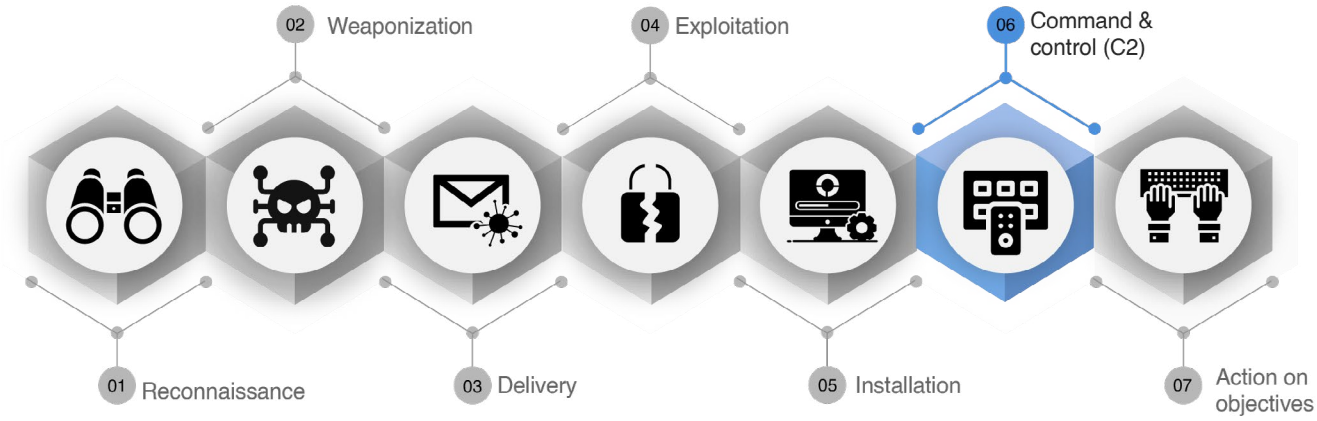
CVE ID	Summary	CVSScore
CVE-2023-34362	In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker 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 effecting 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	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.	9.8
CVE-2023-33299	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.	9.8
CVE-2023-28424	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.	9.8
CVE-2023-32434	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.	7.8
CVE-2023-32435	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.	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 Cl0p portando il gruppo alla compromissione di oltre 150 organizzazioni tra cui compagnie del settore consulting, technology, energy ed hanno 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.

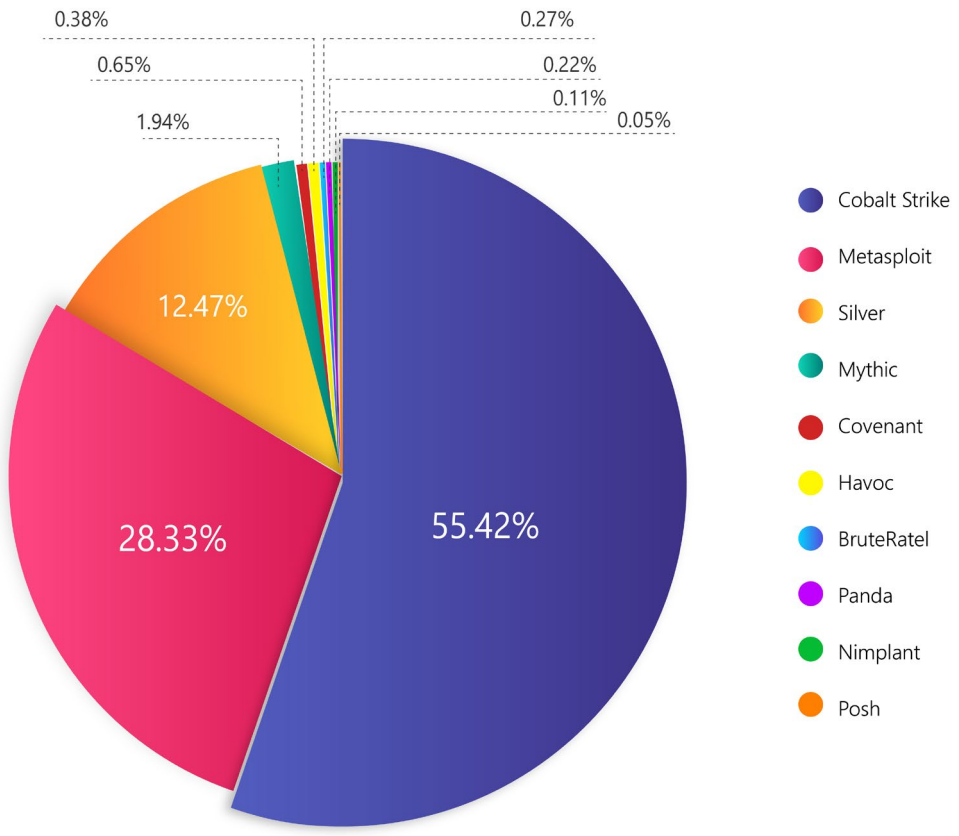
Nel contesto della Cyber Kill Chain, l'installazione di Malware per la comunicazione con un server remoto si colloca nella fase di "Command&Control".

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.

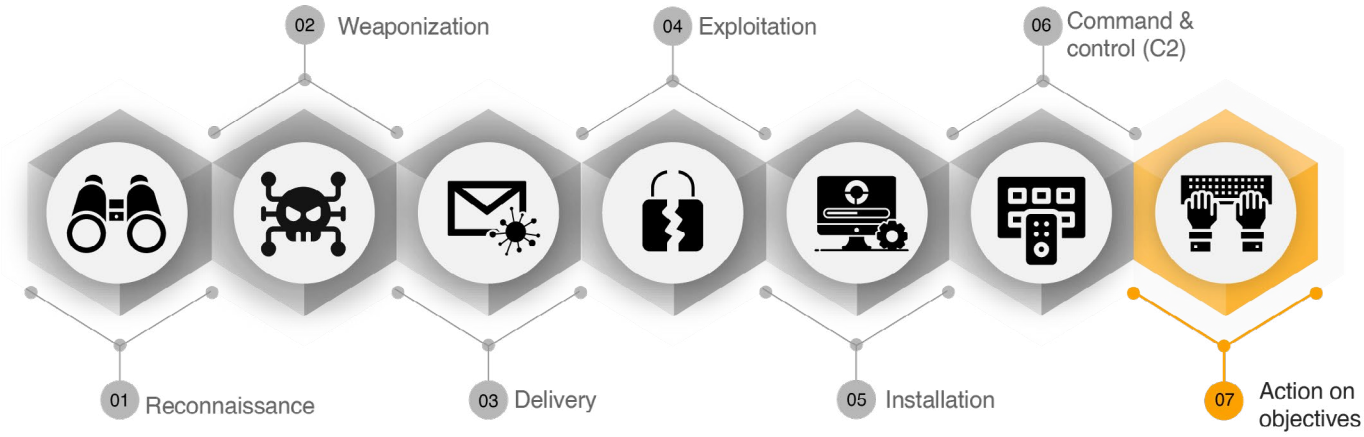
Durante la fase di C2, gli aggressori utilizzano una varietà di tecniche e strumenti per mantenere il controllo sul sistema compromesso e interagire con esso. Questo coinvolge l'uso di malware sofisticati e framework di Command & Control.

Il SME CERT di DIGITAL SME ha identificato i Framework più diffusi durante questo periodo: 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%.

I Framwork più diffusi- Q2 2023



ACTIONS ON OBJECTIVES



Nell'H1 2023 si è registrato un significativo aumento delle vittime colpite da attacchi ransomware, con un totale di 2349 incidenti segnalati in tutto il globo. 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.

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: H1 Summary

La minaccia degli attacchi ransomware continua 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.

Confronto H1 2023 e H1 2022

Key takeaways

Nel corso del primo semestre di quest'anno, abbiamo assistito a un aumento significativo delle vittime di attacchi ransomware in tutto il mondo. Questo dato è allarmante, soprattutto se lo confrontiamo con l'anno precedente. Nel primo semestre del 2022, le vittime di ransomware erano 1.262, mentre nel corso dei primi sei mesi del 2023, tale numero è balzato a 2.349. Questo rappresenta un aumento impressionante del 86.3%, riflesso inequivocabile del continuo sopravanzare del pericolo cyber legato in particolare alle gang ransomware.

A contribuire a questo drammatico incremento sembra essere la gang Lockbit, che ha dimostrato una notevole attività nel periodo in esame. Il loro coinvolgimento in numerosi attacchi ransomware può aver contribuito al brusco aumento delle vittime.

Un altro aspetto che rende questa situazione preoccupante è il fatto che gli attacchi ransomware hanno colpito ben 89 paesi in tutto il mondo. Questo sottolinea la portata globale della minaccia e la necessità di adottare misure di sicurezza informatica efficaci a livello internazionale per proteggere le organizzazioni e gli individui.

Tra tutti i paesi colpiti, gli Stati Uniti emergono come la regione più colpita. Questo potrebbe essere dovuto alla loro vasta presenza digitale e alla loro importanza economica. Gli USA rappresentano un bersaglio allettante per gli attacchi cibernetici, e tale dato dovrebbe sollecitare ulteriormente il governo e le aziende americane a rafforzare le loro difese informatiche.

Attacchi ransomware: Q1 e Q2 confermano il trend di crescita

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.

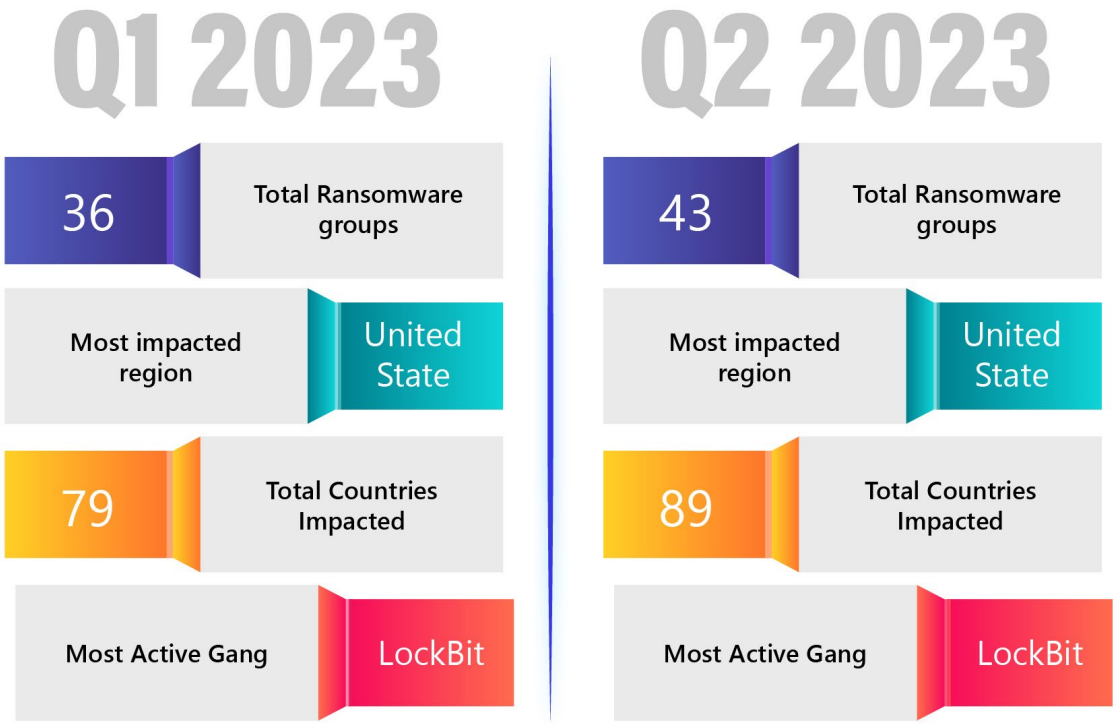
Tuttavia, il Q2 ha visto un ulteriore aumento degli attacchi ransomware, con un totale di 43 gruppi identificati. La regione degli Stati Uniti continua ad essere la più colpita, ma è stato registrato un incremento

significativo 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.

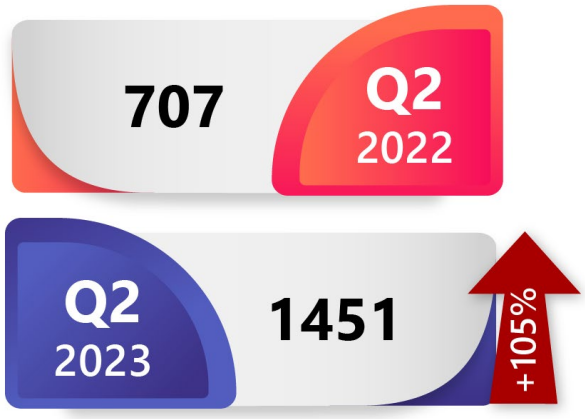
Tra tutti i gruppi di ransomware attivi durante il Q2, LockBit è rimasto il più prolifico e aggressivo, operando su larga scala e colpendo numerose organizzazioni in tutto il mondo.

Numero di Target colpiti dalle gang con data leak.

Confronto Q1 2023 e Q2 2023



Numero di Target colpiti dalle gang con data leak.
Confronto Q2 2022 e Q2 2023



Focus italia (H1)

Guardando il nostro Paese, i dati ci mostrano un interessante andamento nel corso degli anni. Nel primo semestre del 2022, l'Italia aveva registrato **77 vittime** di ransomware, mentre nel primo semestre del 2023 il numero è sceso a **61 vittime**. Questo rappresenta una diminuzione del 20.8% nel numero di vittime rispetto all'anno precedente.

La diminuzione del numero di vittime potrebbe essere il risultato di diversi fattori, tra cui un miglioramento delle misure di sicurezza informatica adottate da organizzazioni italiane, una maggiore consapevolezza delle minacce cibernetiche e delle contromosse da parte delle vittime, o un cambiamento nelle strategie degli attaccanti.

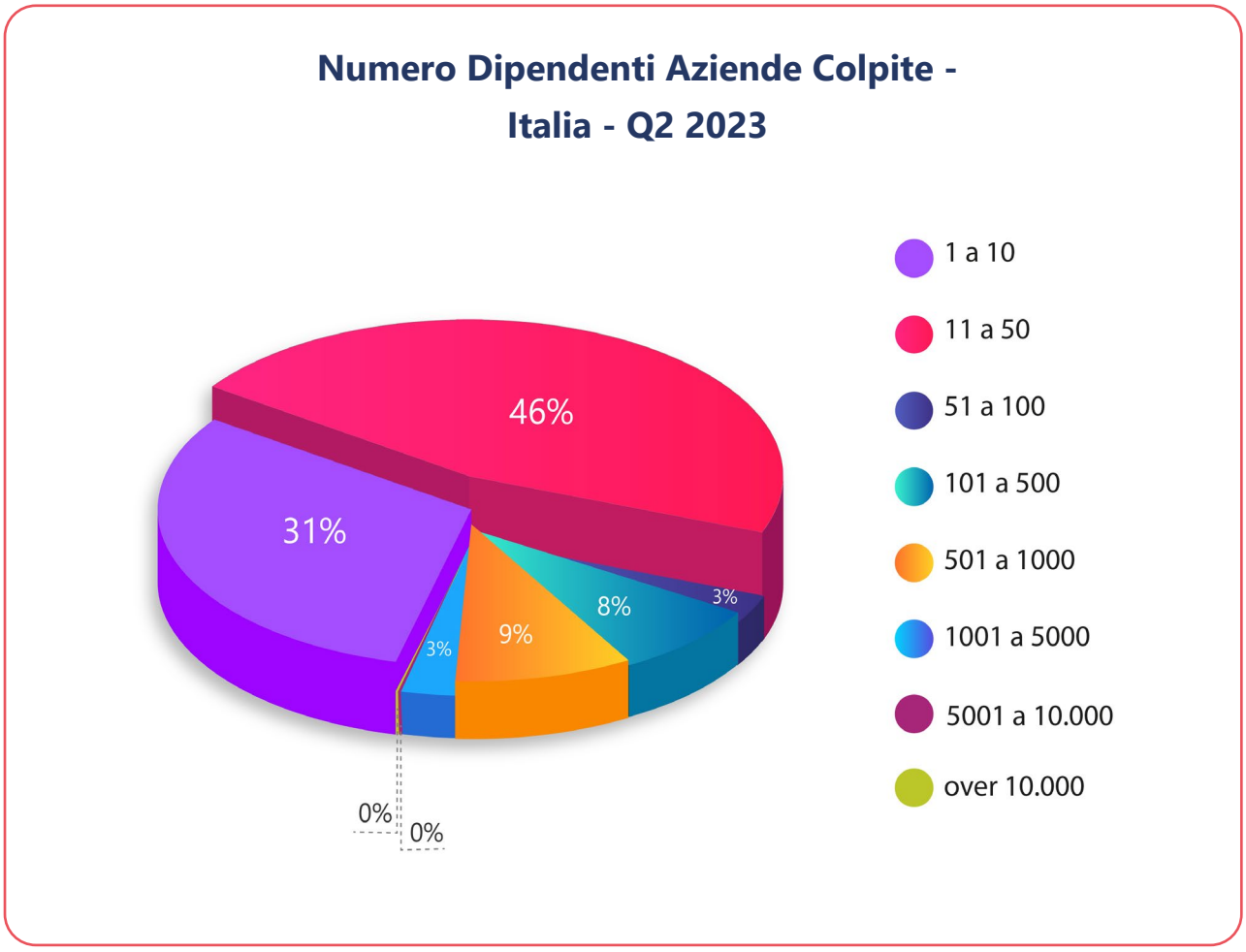
Tuttavia, non possiamo non notare – anche in base alla metodologia di raccolta dati di questa analisi che prende in considerazione unicamente le vittime "confermate" tramite siti di data leak - che le aziende italiane sono spesso associate alla reputazione di essere più propense a pagare il riscatto in caso di attacco ransomware.

Questo potrebbe essere un altro motivo per cui il numero di vittime è diminuito, andando in controtendenza rispetto ad altri paesi. Gli attaccanti potrebbero aver continuato a prendere di mira le organizzazioni italiane sperando in un pagamento del riscatto, ma beneficiando di vittime più propense.

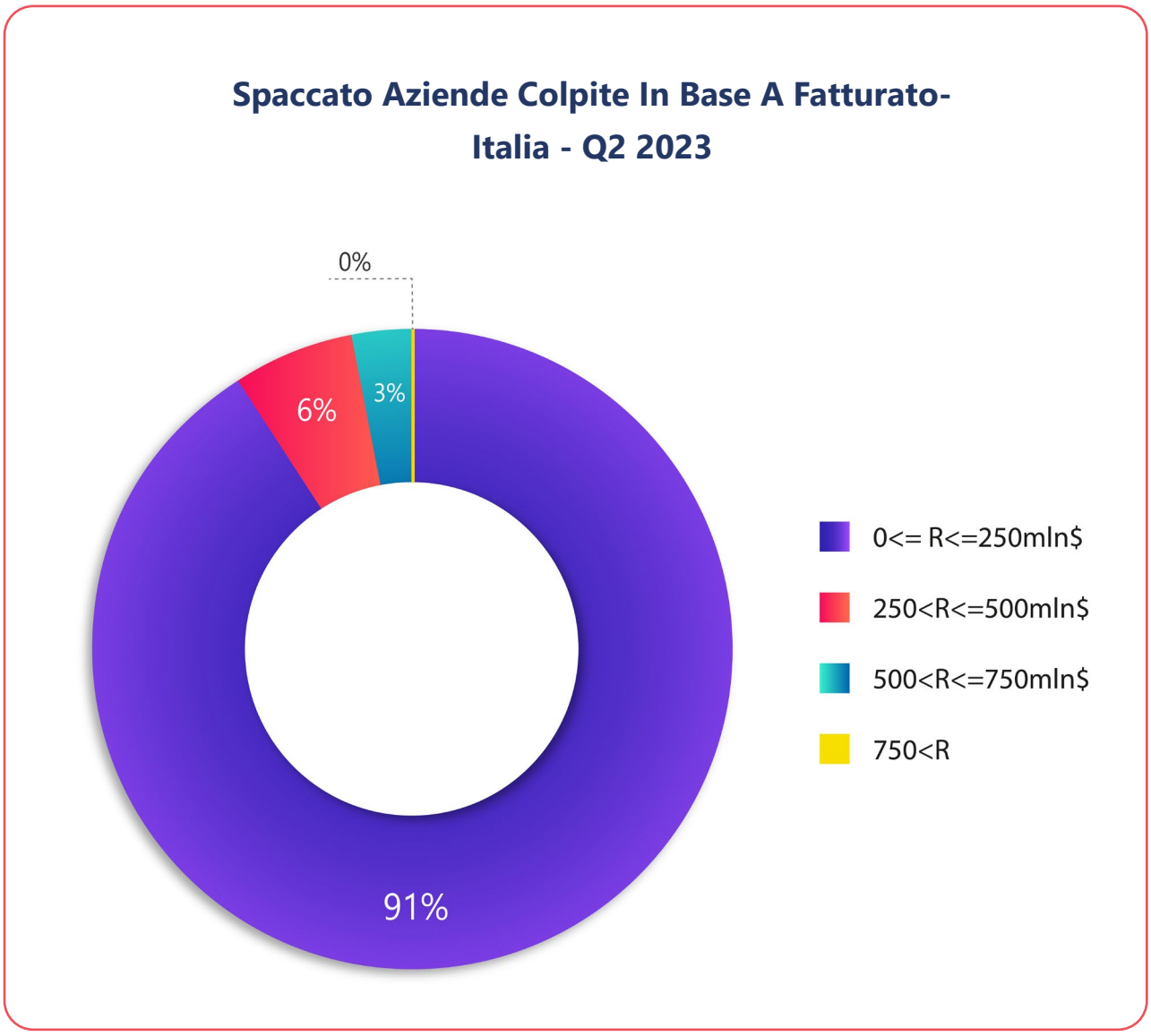
Focus italia (Q2)

Prendendo in esame i dati più recenti, Q2 2023, gli attacchi ransomware in Italia hanno colpito un totale di 35 aziende: di queste, le piccole e medie imprese (PMI) 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 tale 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 rispettivamente l'8% e il 9%. 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.



Nel panorama attuale della cybersecurity in Italia, infatti, le PMI continuano quotidianamente a subire attacchi ransomware. Le statistiche mostrano chiaramente come le aziende con un fatturato fino a 250 milioni di euro 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.



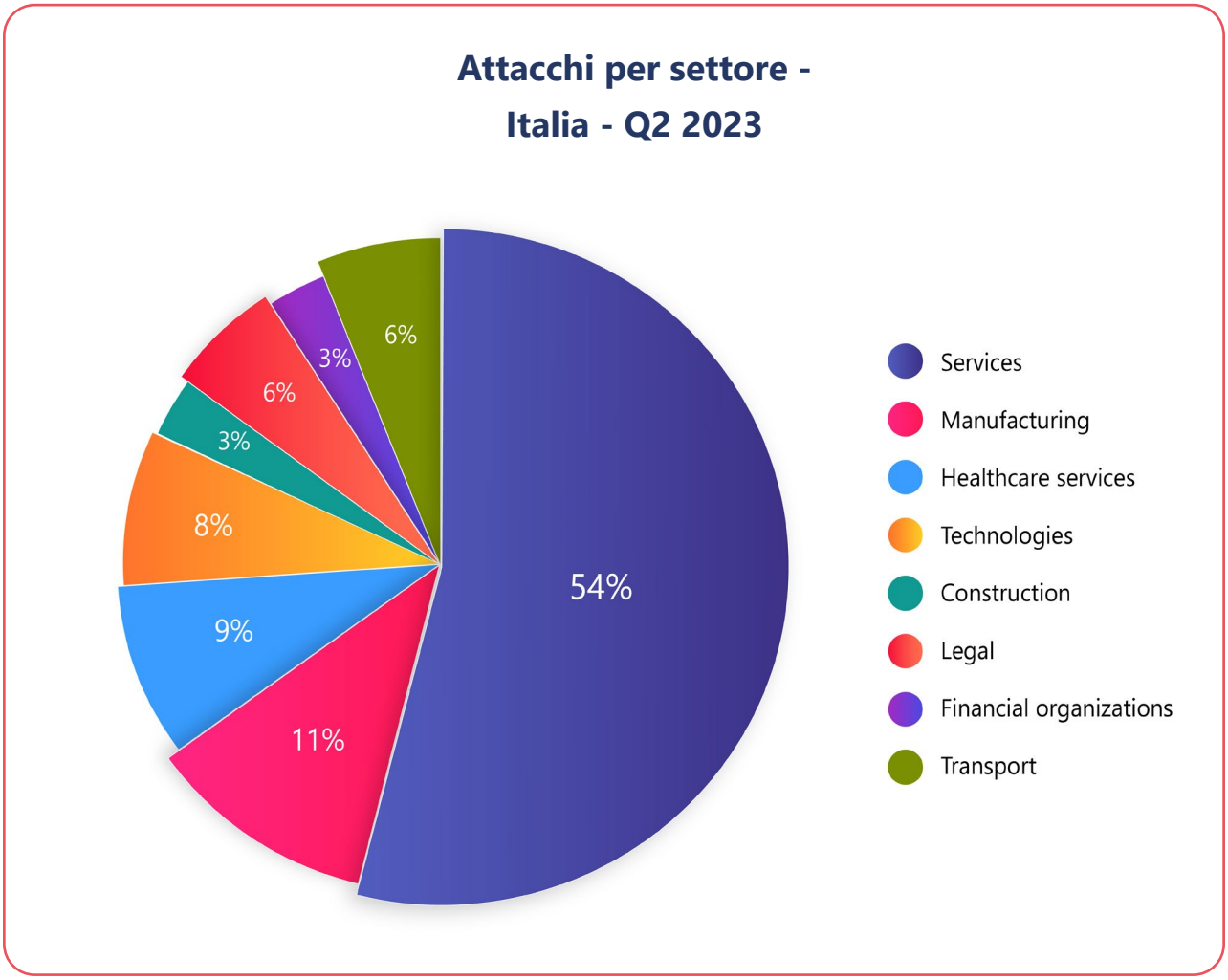
Tra i principali attacchi ransomware in Italia nel Q2 2023, diverse aziende italiane sono state prese di mira dalla gang "Lockbit3", subendo attacchi che hanno messo a repentaglio la sicurezza dei dati e dei sistemi aziendali.

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.

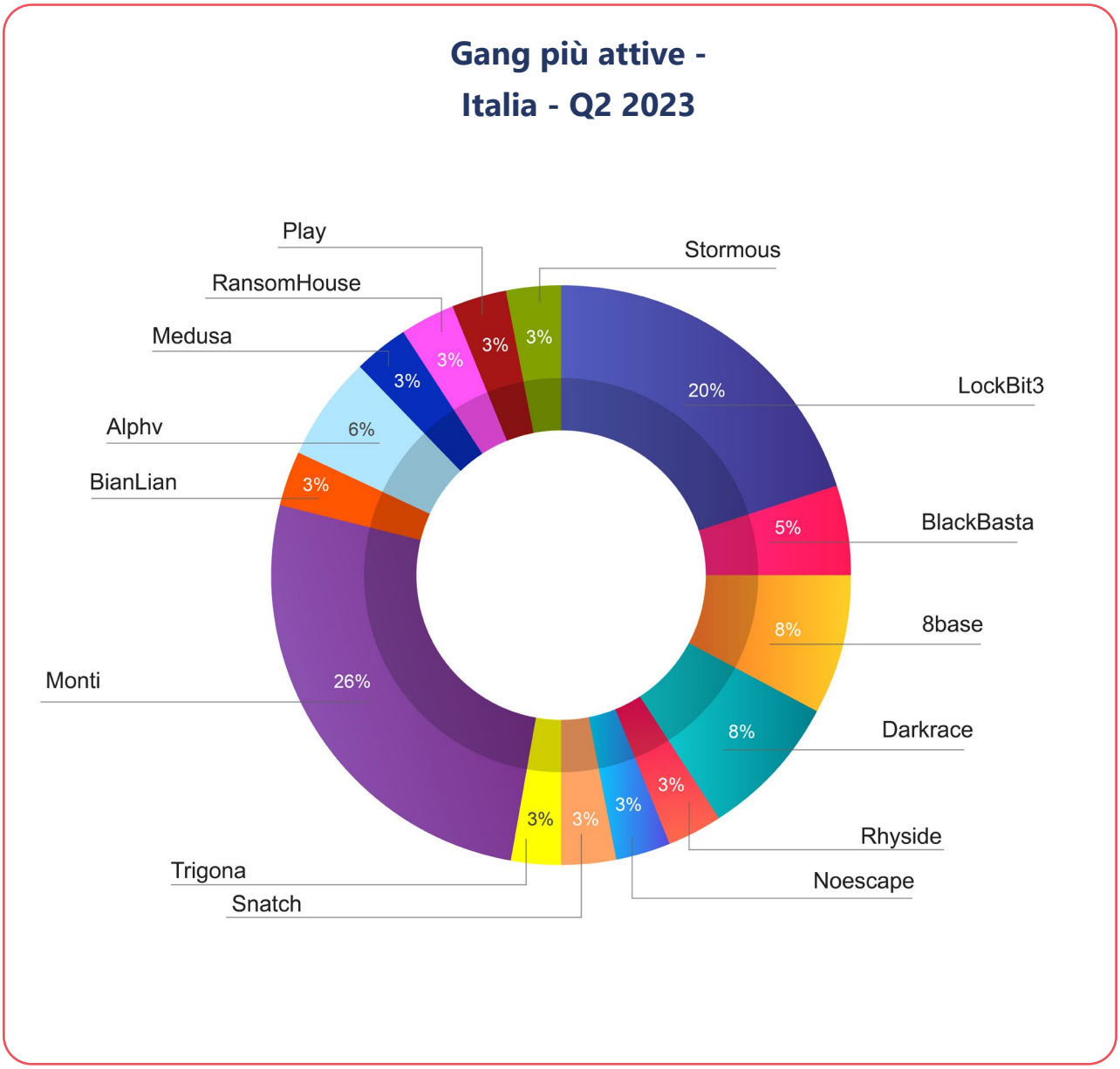
Questi sono solo alcuni degli attacchi ransomware che hanno colpito le imprese italiane nel Q2 2023, evidenziando come nessun settore è immune dagli attacchi informatici: solo attraverso una solida strategia di sicurezza informatica e la consapevolezza dei rischi associati alle minacce informatiche,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



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.



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.

Analysis by:

Swascan, Mediatech, Hackmanac

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