10 YEARS
OF SECURITY INSIGHT

SOTI

V10, NUMERO 05

Affrontare l'ondata:

le tendenze degli attacchi nei servizi finanziari

Akamai

Stato di Internet - Security

Sommario

Introduzione

Il settore dei servizi finanziari non è solo un caposaldo dell'economia globale, ma è la linfa vitale dello sviluppo e della crescita economica. Comprendendo vari settori, come, ad esempio, banche commerciali, responsabili del trattamento dei dati di pagamento, società di gestione patrimoniale, banche per gli investimenti e compagnie di assicurazioni, i servizi finanziari si evolvono in continuazione.

I progressi tecnologici continuano a trasformare lo scenario dei servizi finanziari, dando origine ad innovazioni di tecnologia finanziaria (tecnofinanza), come banche digitali, robo-advisor e risorse crittografiche. Il numero delle società di tecnofinanza è cresciuto enormemente in tutti i paesi del mondo, con Stati Uniti e Cina in cima alla lista. A gennaio 2024, 8 delle più grandi società di tecnofinanza su 10 avevano uffici in questi due paesi. Questa svolta tecnologica si riflette anche nella crescita delle transazioni senza contanti, per le quali si prevede un incremento significativo, soprattutto nei luoghi in cui l'accesso ai servizi finanziari è limitato. Tuttavia, l'innovazione porta con sé inevitabili vulnerabilità.

I criminali informatici prendono incessantemente di mira le istituzioni finanziarie e l'impatto dei loro attacchi supera le perdite economiche. Interruzioni operative, danni alla reputazione e sanzioni normative paralizzanti possono erodere la fiducia su cui si basa il settore dei servizi finanziari. In che modo quindi le istituzioni finanziarie possono stabilire efficaci sistemi di difesa in un momento in cui la velocità della trasformazione digitale è paragonabile solo alla complessità delle minacce informatiche?

Questo rapporto sullo stato di Internet è stato concepito specificamente per aiutare i professionisti che operano nel settore dei servizi finanziari in tutto il mondo (clienti di Akamai, ricercatori della cybersicurezza e leader del settore) a muoversi nello scenario delle minacce sempre più complesso. Il settore dei servizi finanziari, che è l'obiettivo principale dei criminali informatici, richiede uno sforzo collaborativo per salvaguardare la sua infrastruttura critica, proteggere aziende e clienti, garantire la stabilità dei mercati finanziari e prevenire problemi economici. La ricerca presentata in questo rapporto è rivolta a coloro che desiderano tenersi al passo con gli autori degli attacchi, rafforzare le risorse critiche del settore e garantire un continuo livello di fiducia e affidabilità a supporto delle relazioni finanziarie a livello globale.

Rafforzare i servizi finanziari con la conformità, la resilienza operativa e la cybersicurezza

Una delle sfide centrali che oggi si trova ad affrontare il settore dei servizi finanziari è la necessità di migliorare la conformità e la resilienza operativa. Man mano che lo scenario delle normative si evolve, le istituzioni finanziarie devono adattarsi in modo proattivo per soddisfare queste nuove richieste. L'introduzione del DORA (Digital Operational Resilience Act), ad esempio, sottolinea la necessità di adottare un solido sistema in grado di resistere alle interruzioni dei servizi ICT (Information and Communication Technology). Il DORA, che entrerà in vigore a gennaio 2025, obbliga gli enti finanziari e i loro provider di servizi di terze parti ad adottare strategie di resilienza complete, spingendo le aziende a migliorare le loro funzionalità di sicurezza e risposta agli incidenti.

Le linee guida aggiornate della U.S. Securities and Exchange Commission amplificano ulteriormente la necessità di adottare un approccio olistico alla cybersicurezza. Le istituzioni finanziarie ora devono integrare la resilienza operativa e il disaster recovery nelle loro strategie, ponendo una particolare enfasi sugli aspetti materiali dei rischi informatici, il che implica una profonda comprensione del modo con cui minacce e incidenti significativi possono influire sulla stabilità e sulle operazioni finanziarie. L'obbligo di dover pubblicare tempestivamente nei rapporti annuali gli incidenti materiali di cybersicurezza e le strategie di gestione dei rischi articolate in modo dettagliato indica un cambio di paradigma nelle aspettative in materia di normative. Per muoversi in questi scenari normativi, le istituzioni finanziarie devono collaborare con aziende in grado di offrire visibilità e soluzioni per la sicurezza all'avanguardia. Come mostrato in questa ricerca, le competenze di Akamai possono aiutare a garantire che le società di servizi finanziari non solo riescano a soddisfare i requisiti di conformità, ma anche a mantenere l'integrità operativa tra le rigorose normative vigenti.

Considerando questi sviluppi, le istituzioni finanziarie devono adottare un approccio completo per risolvere le complessità dei processi di conformità e della resilienza operativa, incluse le operazioni di identificazione e prioritizzazione dei rischi materiali, che cioè possono influire in modo significativo sul processo decisionale di un investitore. Le istituzioni finanziarie devono integrare questi rischi materiali nei loro sistemi di gestione dei rischi e garantire che vengano messi in atto solidi piani di risposta agli incidenti. Il percorso verso un'efficace resilienza operativa si basa sull'adozione di una strategia di difesa approfondita multilivello, che include la riduzione della superficie di attacco tramite la segmentazione di rete e la microsegmentazione, l'implementazione della crittografia dei dati inattivi, il rafforzamento dei server e l'utilizzo di soluzioni WAF (Web Application Firewall) insieme ad avanzati sistemi di rilevamento delle minacce. Il monitoraggio continuo e le valutazioni regolari sulla sicurezza sono cruciali per identificare e mitigare i rischi tempestivamente.

Gli esercizi nella pianificazione della risposta agli incidenti, basati sulle attuali ricerche e sull'intelligence sulle minacce, come i rapporti sullo stato di Internet (SOTI) di Akamai, sono essenziali per le istituzioni finanziarie perché aiutano a costruire scenari plausibili e a garantire che le istituzioni possano adattarsi a nuovi strumenti, tecniche e procedure man mano che si rendono disponibili. Questo approccio proattivo è vitale per garantire la resilienza operativa e per mantenere la fiducia dei clienti in uno scenario delle minacce sempre più volatile. Man mano che il settore dei servizi finanziari si evolve, l'intersezione di conformità, resilienza operativa e cybersicurezza continuerà a trasformare il suo futuro. Adottando avanzate misure di sicurezza e migliorando il loro livello di visibilità, le istituzioni finanziarie possono affrontare le complessità normative e salvaguardare le loro attività per mantenere la fiducia che è essenziale nelle nostre attività aziendali.

Teresa Walsh
Global Head of Intelligence, FS-ISAC

Informazioni chiave

34%

Percentuale di attacchi DDoS ai livelli 3 e 4 subiti dalle società di servizi finanziari

I servizi finanziari rimangono il settore maggiormente colpito dagli attacchi DDoS (Distributed Denial-of-service) ai livelli 3 e 4, seguiti dal gaming (18%) e dall'high-tech (15%). Queste minacce prevalenti derivano probabilmente dalle attuali tensioni geopolitiche, in particolar modo dalla guerra tra Russia e Ucraina e dal conflitto tra Israele e Hamas, che hanno favorito un'impennata delle attività degli hacktivisti in tutto il mondo.

La crescita delle API favorisce l'aumento degli attacchi DDoS al livello 7

Anche se le applicazioni web sono tradizionalmente gli obiettivi privilegiati degli attacchi informatici, gli attacchi DDoS al livello 7 sferrati contro le API fanno registrare picchi notevoli durante il periodo osservato nel rapporto, che sono principalmente dovuti alla crescente adozione delle API nei servizi finanziari per soddisfare i requisiti normativi e di conformità in continua evoluzione. Poiché le organizzazioni si affidano sempre più alle API, i criminali stanno adattando le loro tattiche, il che rende la sicurezza delle API una delle massime priorità per le aziende moderne.

I picchi di traffico evidenziano la necessità di valutare gli attacchi DDoS in base alla frequenza e al volume

Gli attacchi DDoS contro i servizi finanziari rivelano un dato di importanza critica: la frequenza degli attacchi non è sempre correlata con la loro intensità. Anche se alcuni mesi mostrano la presenza di pochi attacchi, i corrispondenti dati dei Gbps indicano significativi picchi di traffico, il che sottolinea la necessità di considerare il volume e la frequenza degli attacchi al momento di valutare l'impatto degli attacchi DDoS.

36%

Percentuale di domini sospetti che prendono di mira le istituzioni finanziarie

Gli attacchi di phishing prendono sempre più di mira i clienti dei servizi finanziari, facendo aumentare il rischio di subire furti delle identità e attacchi per il controllo degli account. Questa tendenza negli attacchi espone le istituzioni finanziarie ad una maggiore attenzione da parte delle autorità di regolamentazione e le violazioni sollevano preoccupazioni tra i clienti minando la loro fiducia.

30%

Percentuale di pagine visitate su siti di phishing e impersonificazione dei brand

I criminali riescono ad indirizzare il traffico dei clienti verso siti fraudolenti imitando app e servizi finanziari legittimi. Inoltre, continuano a prendere di mira le istituzioni finanziarie con gli attacchi di phishing per estrapolare le grandi quantità di informazioni sensibili di cui dispongono queste organizzazioni.

I servizi finanziari rimangono il primo settore per numero di attacchi DDoS ai livelli 3 e 4

Gli attacchi DDoS (Distributed Denial-of-Service) ai livelli 3 e 4 prendono di mira i livelli di rete e trasporto, sovraccaricando l'infrastruttura di rete ed esaurendo la larghezza di banda e le risorse del server. Questi attacchi inviano enormi quantità di traffico allo scopo di esaurire la capacità della rete e di peggiorare le performance per gli utenti legittimi. Tra tutti i settori esaminati, i servizi finanziari sono l'obiettivo principale degli attacchi DDoS ai livelli 3 e 4 (Figura 1). Questa tendenza è favorita da vari fattori interconnessi che hanno creato una bufera perfetta di vulnerabilità e opportunità per i criminali.

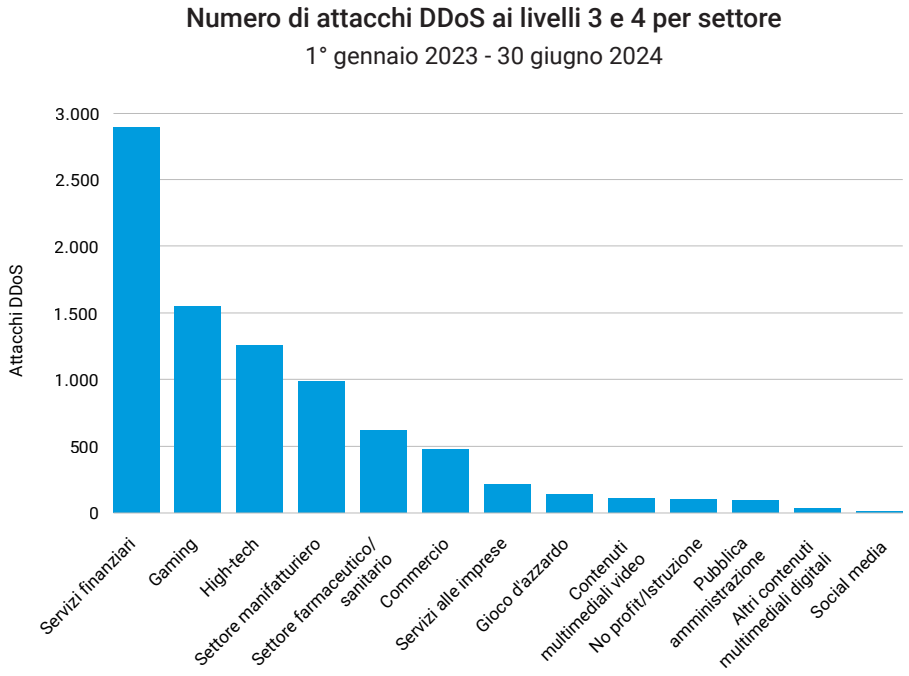


Figura 1. Il settore dei servizi finanziari primeggia sugli altri settori per numero di attacchi DDoS ai livelli 3 e 4

Le tensioni geopolitiche hanno svolto un ruolo significativo nell'aumento degli attacchi DDoS sferrati contro le istituzioni finanziarie. La guerra tra Russia e Ucraina e il conflitto tra Israele e Hamas, tutt'ora in corso, sono coincisi con un notevole aumento delle attività degli hacktivisti filorussi e filopalestinesi. Questi conflitti hanno favorito un'impennata degli attacchi DDoS, specialmente quelli sferrati contro le banche europee che hanno rapporti con l'Ucraina. Le motivazioni politiche alla base di questi attacchi aggiungono un ulteriore livello di complessità alla scenario delle minacce.

Le istituzioni finanziarie sono bersagli particolarmente allettanti per gli autori di attacchi DDoS a causa dell'elevata posta in gioco. Un'interruzione delle attività aziendali può causare un grave impatto finanziario, notevoli danni alla reputazione e la perdita di fiducia nel sistema finanziario globale. Il potenziale di diffusione delle conseguenze rende i servizi finanziari l'obiettivo principale per chi cerca di causare interruzioni importanti o divulgare dichiarazioni politiche.

I progressi tecnologici hanno aumentato notevolmente la potenza e le capacità degli autori degli attacchi DDoS, che ora possono utilizzare le botnet delle macchine virtuali (VM) per sferrare attacchi in modo più efficiente sfruttando le risorse di elaborazione disponibili su vari dispositivi IoT (Internet of Things) e VM. Questo approccio sfrutta la natura distribuita dei servizi cloud, rendendo gli attacchi più difficili da mitigare e da monitorare. I criminali possono trarre vantaggio dall'elevata disponibilità della larghezza di banda e dalle vaste risorse computazionali per sferrare attacchi DDoS adattabili, potenti ed economicamente vantaggiosi con varie strategie.

La crescente superficie di attacco nel settore dei servizi finanziari ha, inoltre, contribuito all'aumento degli attacchi DDoS. Il crescente uso dei servizi digitali e delle API ha creato più punti di ingresso per i criminali. Questa svolta ha aggiunto complessità ai sistemi finanziari e ha introdotto varie vulnerabilità che i criminali possono sfruttare. Destano particolare preoccupazione le API ombra non documentate, che, spesso, non sono protette perché i team addetti alla sicurezza delle informazioni non sanno della loro esistenza. I criminali possono sfruttare queste API per esfiltrare i dati, bypassare i controlli di autenticazione o eseguire azioni di disturbo.

Le pressioni normative hanno inavvertitamente incrementato la vulnerabilità delle istituzioni finanziarie nei confronti degli attacchi DDoS. Requisiti come la direttiva PSD2 (Payment Services Directive 2), introdotta dall'Unione europea, hanno obbligato le banche a rendere accessibili i loro sistemi a provider di servizi di terze parti, come le società di tecnofinanza, tramite le API. Anche se, in tal modo, le banche possono rispondere alle crescenti aspettative dei clienti tramite l'integrazione con la tecnofinanza, le app mobili e altre piattaforme, i rischi per la sicurezza sono aumentati e la superficie di attacco è diventata più ampia. Il crescente uso delle API tra queste varie entità ha creato più potenziali point of failure che i criminali possono prendere di mira.

Insieme, questi fattori hanno contribuito a far rimanere il settore dei servizi finanziari l'obiettivo principale degli attacchi DDoS ai livelli 3 e 4. La combinazione di motivazioni geopolitiche, obiettivi di alto valore, progressi tecnologici, un contesto sempre più digitale e le pressioni normative ha creato un ambiente in cui gli attacchi DDoS contro le istituzioni finanziarie non solo sono più frequenti, ma anche potenzialmente più devastanti che mai prima d'ora. Parallelamente alla continua evoluzione del settore, devono evolversi anche i suoi sistemi di difesa da queste minacce sempre più sofisticate e persistenti.

I criminali possono trarre vantaggio dall'elevata disponibilità della larghezza di banda e dalle vaste risorse computazionali per sferrare attacchi DDoS adattabili, potenti ed economicamente vantaggiosi con varie strategie.

Gli attacchi DDoS ai livelli 3 e 4: un giro sulle montagne russe

Anche se il settore dei servizi finanziari subisce gli attacchi DDoS ai livelli 3 e 4 con maggiore frequenza rispetto agli altri settori, il numero di questi attacchi varia nel corso dell'anno (Figura 2).

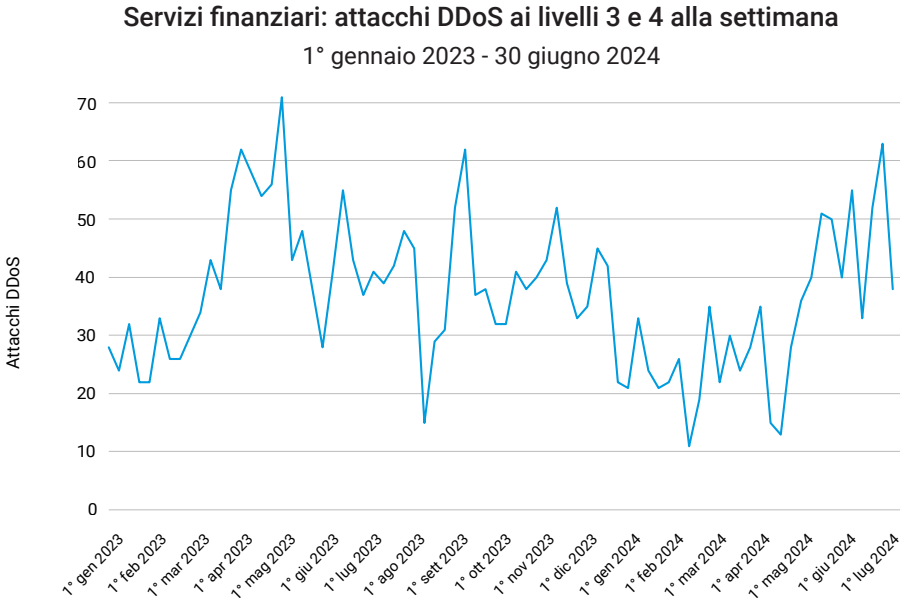


Figura 2. L'aumento e la diminuzione degli attacchi DDoS ai livelli 3 e 4 nel settore dei servizi finanziari

Gli attacchi DDoS ai livelli 3 e 4 sferrati contro il settore dei servizi finanziari nei periodi di marzo/aprile 2023, agosto/settembre 2023 e aprile/maggio 2024 si possono attribuire a vari fattori specifici.

Negli Stati Uniti, la primavera (da marzo ad aprile) è il periodo di presentazione della denuncia dei redditi, pertanto rappresenta un'allettante opportunità per gli autori degli attacchi DDoS. Si è verificato un considerevole aumento di attacchi per l'abuso dei conti in banche nazionali e locali a partire dal 16 aprile, data che coincide con il giorno in cui molte banche comunicano i loro guadagni del primo trimestre dell'anno. In questo periodo, i provider di servizi di rete e di gestione delle identità e degli accessi (IAM), come Okta e Cisco, hanno segnalato anche un notevole incremento nel numero di attacchi di credential stuffing sferrati contro i servizi online.

Ad aprile 2023, nello specifico, l'individuazione di una vulnerabilità molto grave nel protocollo SLP (Service Location Protocol), la CVE-2023-29552, ha probabilmente contribuito all'impennata delle attività degli attacchi. Sembra che questa vulnerabilità, che può amplificare gli attacchi DDoS sia a livello di rete che a livello di applicazioni, abbia interessato più di 2.000 organizzazioni in tutto il mondo e oltre 54.000 istanze SLP su Internet. Sfruttando questa vulnerabilità, i criminali potrebbero usare le istanze violate per sferrare attacchi di amplificazione DDoS su larga scala. Con un fattore di amplificazione fino a 2.200 volte, questa vulnerabilità ha consentito di lanciare uno degli attacchi di amplificazione più significativi mai documentati.

Abbiamo identificato un attacco importante esaminando il periodo di agosto/settembre 2023. Akamai ha osservato e contrastato l'attacco DDoS più grande mai registrato, che è stato sferrato contro un'istituzione finanziaria negli Stati Uniti il 5 settembre 2023. Questo attacco ha combinato le tecniche ACK, PUSH, RESET, and SYN flood, raggiungendo picchi di intensità pari a 633,7 gigabit al secondo (Gbps) e 55,1 milioni di pacchetti al secondo (Mpps). Nonostante la sua elevata intensità, l'attacco è stato breve, della durata di meno di due minuti.

Focus sulla sicurezza

L'intensità degli attacchi DDoS ai livelli 3 e 4: confronto tra numero di attacchi e valori in Gbps

Per comprendere pienamente la minaccia posta dagli attacchi DDoS sul settore dei servizi finanziari, è fondamentale capirne l'estrema complessità e la portata. Non si tratta di semplici incidenti isolati: ogni attacco, spesso, comporta più tentativi di volume elevato che inondano le reti con gigabit di dati e milioni di pacchetti al secondo. La complessità, l'intensità e la durata degli attacchi stanno aumentando e i criminali utilizzano tecniche più varie, che aumentano i rischi per le istituzioni finanziarie (Figura 3).

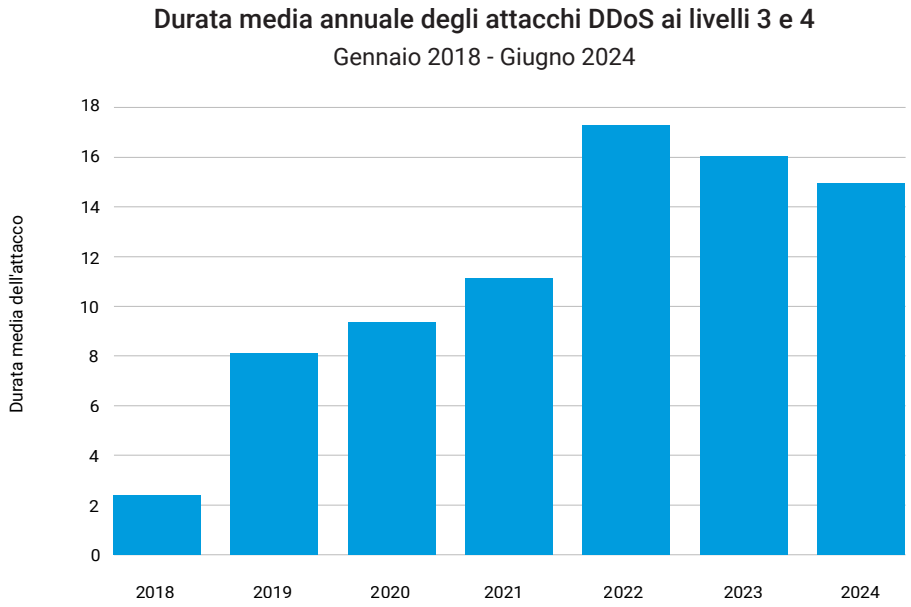


Figura 3. La tendenza globale vede aumentare la durata degli attacchi DDoS ai livelli di 3 e 4

Inoltre, se confrontiamo il grafico relativo al numero di attacchi DDoS ai livelli 3 e 4 nel settore dei servizi finanziari con i corrispondenti dati dei Gbps relativi agli attacchi DDoS, possiamo notare una notevole discrepanza (Figura 4). Il grafico dei Gbps mostra valori nettamente aumentati che non sono presenti nel grafico degli attacchi. Questa disparità evidenzia un concetto importante: anche un mese con un numero di attacchi relativamente ridotto può comunque registrare un volume altissimo di traffico di attacchi DDoS in termini di Gbps.

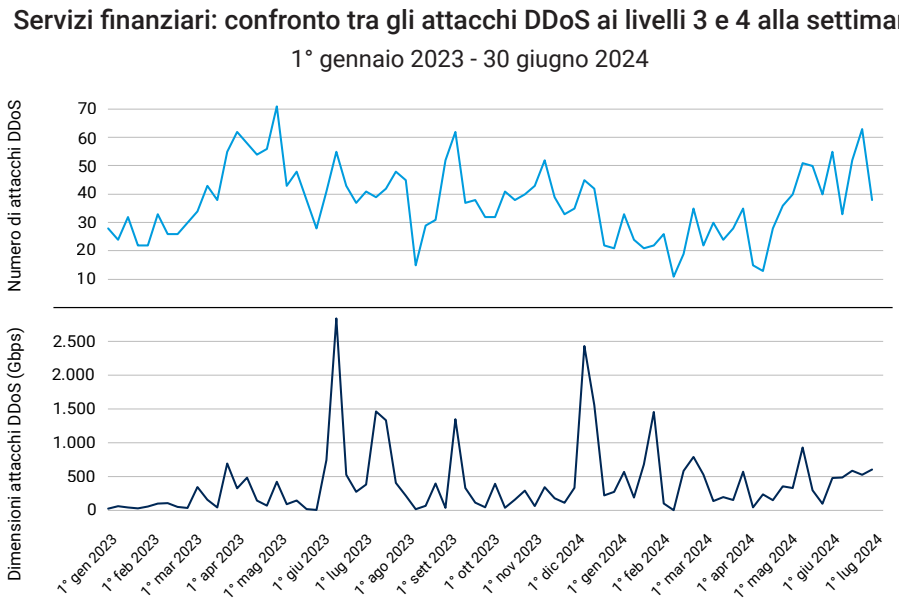


Figura 4. Confronto tra il numero di attacchi DDoS ai livelli 3 e 4 contro il settore dei servizi finanziari e i loro valori in Gbps

Questa osservazione evidenzia un punto critico: basarsi esclusivamente sulla frequenza degli attacchi sottovaluta seriamente la reale minaccia. È, pertanto, essenziale considerare sia il volume che l'intensità del traffico in ogni attacco. Un esiguo numero di attacchi DDoS ad alta intensità può causare molti più danni rispetto ad un gran numero di attacchi di portata minore, il che rende imprescindibile valutare l'intera entità di ogni minaccia.

Una tendenza ad agire in solitaria: gli attacchi DDoS ai livelli 3 e 4 a vettore singolo contro i servizi finanziari

Gli attacchi multivettore sferrati contro le applicazioni o le reti sono una strategia utilizzata comunemente dai criminali informatici che tentano di corrompere o di ottenere l'accesso non autorizzato ad un sistema. Tuttavia, i criminali che mirano in particolare al settore dei servizi finanziari sembrano utilizzare più frequentemente un vettore singolo negli attacchi DDoS ai livelli 3 e 4 (Figura 5).

Tipo di vettori utilizzati negli attacchi DDoS ai livelli 3 e 4 per numero di attacchi

1° gennaio 2023 - 30 giugno 2024

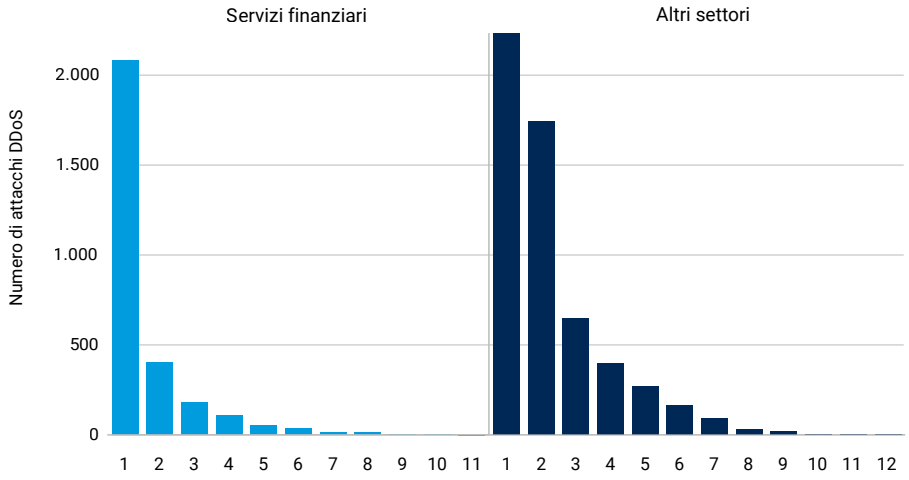


Figura 5. Gli attacchi a vettore singolo sono usati più ampiamente negli attacchi DDoS ai livelli 3 e 4 contro i servizi finanziari

Gli attacchi DDoS a vettore singolo che prendono di mira i livelli 3 e 4 richiedono un minor numero di risorse e possono risultare altamente efficaci di per sé, specialmente contro le istituzioni finanziarie che potenzialmente dispongono di solidi sistemi di difesa dagli attacchi più complessi. Gli attacchi a vettore singolo sono, di solito, più semplici da eseguire e richiedono una minore coordinazione rispetto agli attacchi multivettore. Inoltre, alcune vulnerabilità note presenti ai livelli 3 e 4 delle istituzioni finanziarie potrebbero venire sfruttate in modo efficace con un attacco a vettore singolo senza il rischio di tentare altri tipi di vettori che i sistemi di sicurezza potrebbero, invece, rilevare.

Questa preferenza per gli attacchi a vettore singolo nel settore dei servizi finanziari rappresenta un problema specifico per i team addetti alla cybersicurezza. Anche se dovete rimanere vigili per difendervi dai complessi attacchi multivettore, è fondamentale garantire che i sistemi di difesa riescano a resistere agli attacchi ai livelli 3 e 4 a vettore singolo.

Aumento degli attacchi DDoS al livello 7 contro le API

Gli attacchi DDoS a livello di applicazione (livello 7), anche noti come attacchi HTTP o al livello del traffico web, sono diventati prevalenti e ora sono il metodo preferito dai criminali che prendono di mira il settore dei servizi finanziari. Questi attacchi si focalizzano soprattutto sui componenti delle applicazioni che utilizzano un maggior numero di risorse, negando di fatto l'accesso agli utenti legittimi. A differenza degli attacchi DDoS ai livelli 3 e 4, che spesso sono mitigati dalla protezione dei firewall e della rete, gli attacchi al livello 7 bypassano questi sistemi di difesa spacciandosi per richieste legittime quando prendono di mira funzioni di ricerca o pagine di applicazioni specifiche con l'obiettivo di sovraccaricare il server delle applicazioni.

Anche se le applicazioni web nel settore dei servizi finanziari sono, generalmente, state colpite più frequentemente rispetto alle API, abbiamo osservato un netto aumento nel numero di attacchi DDoS al livello 7 che hanno preso specificamente di mira le API (Figura 6). Questi picchi sono notevolmente più vari e significativi rispetto al modello complessivo degli attacchi alle API sferrati contro altri settori.

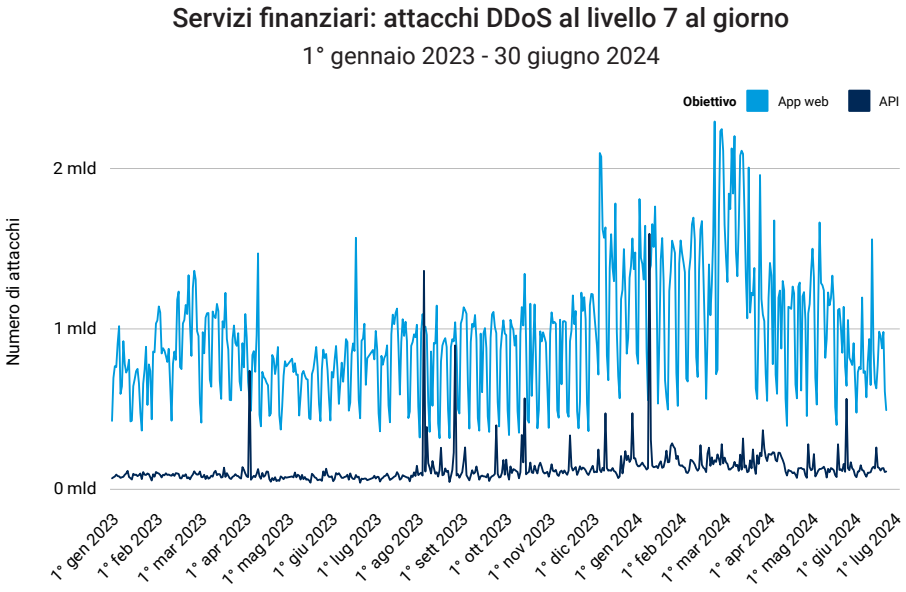
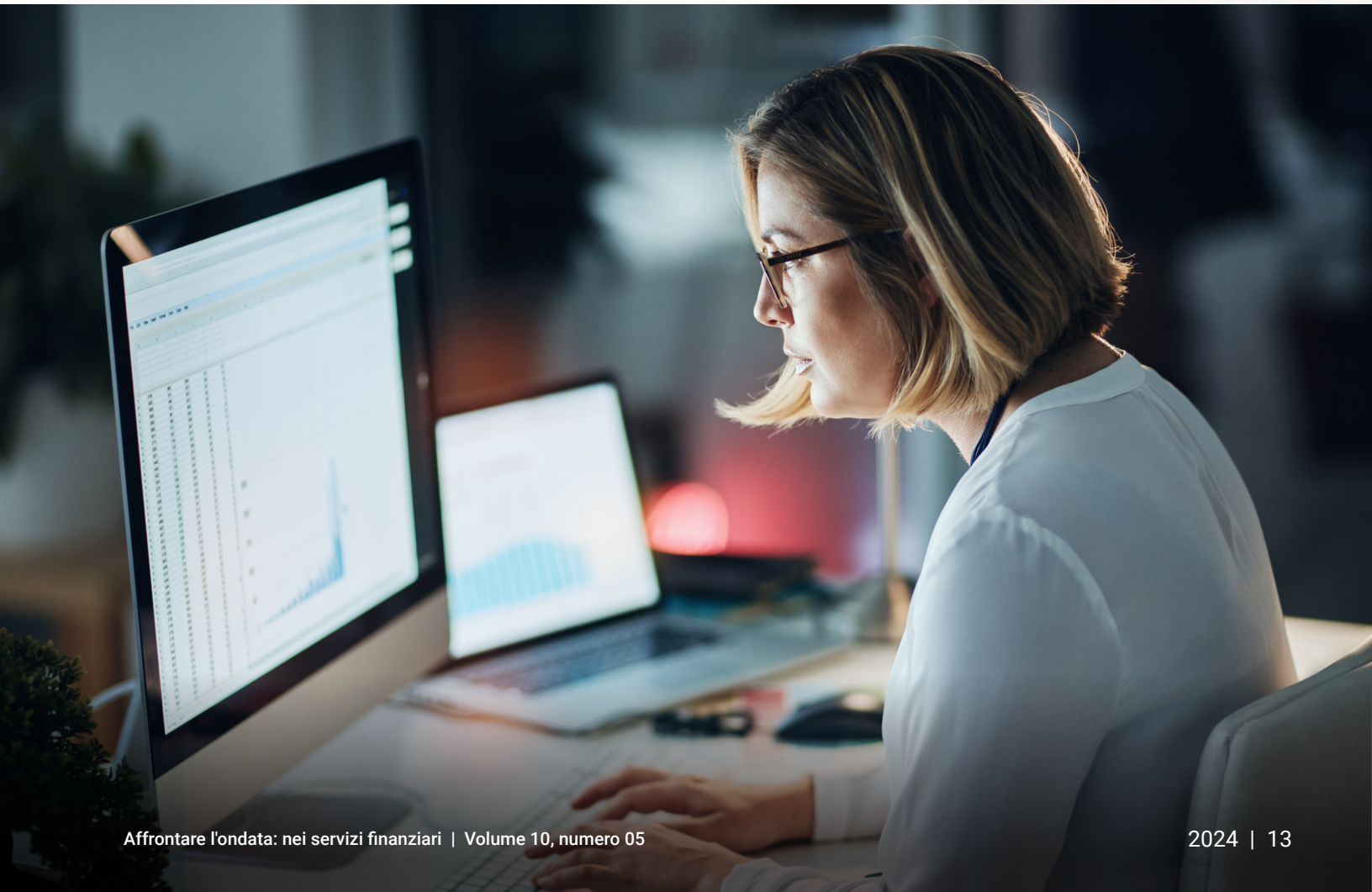


Figura 6. I modelli degli attacchi variano notevolmente tra le API e le applicazioni web prese di mira negli attacchi DDoS al livello 7 contro il settore dei servizi finanziari

Questi valori nettamente aumentati si sono verificati, nello specifico, ad aprile 2023, ad agosto 2023 e a gennaio 2024. Secondo noi, questi picchi sono da attribuire a fattori simili a quelli che influiscono sugli attacchi ai livelli 3 e 4, insieme ad altri elementi specifici del livello 7.

I criminali cercano continuamente nuove vulnerabilità da sfruttare e l'individuazione di tali punti deboli può condurre ad aumenti improvvisi nella frequenza degli attacchi. Ad esempio, la vulnerabilità HTTP/2 Rapid Reset (CVE-2023-44487), identificata per la prima volta ad agosto 2023, è stata sfruttata per sferrare attacchi DDoS a livello 7 altamente efficaci. Questa vulnerabilità ha consentito ai criminali di sfruttare la logica apparentemente legittima e di raggruppare più richieste in un flusso, che ha sovraccaricato server e applicazioni. Ne è risultato il più imponente attacco DDoS al livello 7 mai registrato fino ad oggi.

Inoltre, gli attacchi DDoS basati su eventi stagionali rimangono una tattica comunemente utilizzata dai criminali informatici che prendono di mira le istituzioni finanziarie, con picchi notevoli durante i periodi delle dichiarazioni fiscali e delle vacanze. L'aumento significativo registrato a gennaio 2024, in seguito alla corsa agli acquisti natalizi, suggerisce che i criminali si stavano preparando per sferrare il loro attacco durante i periodi caratterizzati da un maggior numero di transazioni online.



Il ransomware e l'hacktivismo nei servizi finanziari

Il settore dei servizi finanziari è spesso preso di mira da criminali altamente sofisticati, come i gruppi di ransomware. Questi gruppi utilizzano un'ampia gamma di tecniche per penetrare nelle istituzioni finanziarie, rubare informazioni sensibili e richiedere grandi somme di denaro come riscatto. Sebbene questi gruppi siano animati da motivazioni principalmente economiche, possono anche risentire dei contesti geopolitici prendendo di mira le istituzioni finanziarie che hanno legami politici, come nel caso del gruppo di ransomware i stanza in Russia noto come REvil (chiamato anche Sodinokibi). Anche il gruppo BlackCat (ALPHV) è stato coinvolto in questo modo, come si è visto nei suoi attacchi contro un'importante banca.

Uno dei gruppi di ransomware più attivi, noto per i suoi attacchi sferrati contro organizzazioni di grandi dimensioni, tra cui istituzioni finanziarie, continua a rimanere il gruppo LockBit, nonostante la recente stretta delle forze dell'ordine. L'Operazione Cronos, in cui le agenzie Europol e Eurojust hanno collaborato per la prima volta per coordinare una task force internazionale, è stata superata da una nuova infrastruttura stabilita dal gruppo LockBit. Questo gruppo di ransomware è riemerso con una nuova infrastruttura e un sito sul dark web dopo che l'operazione condotta dalle forze dell'ordine aveva sequestrato i suoi server a febbraio 2024. Inoltre, il gruppo LockBit ha dichiarato che sarebbe passato alla controffensiva aumentando i suoi attacchi contro le reti governative in risposta all'Operazione Cronos.

Anche il gruppo di ransomware CL0P continua a rimanere attivo ed è noto specialmente per la sua capacità di sfruttare le vulnerabilità presenti nei software di trasferimento dei file ampiamente usati dalle organizzazioni, tra cui le istituzioni finanziarie. Un esempio significativo è rappresentato dalla vulnerabilità zero-day a cui è stato assegnato il codice CVE-2023-34362, che ha interessato il software MOVEit Transfer ed è iniziata con un attacco SQL injection sferrato per penetrare nell'applicazione web MOVEit Transfer. Almeno 15 banche e cooperative di credito hanno confermato di aver subito una violazione di dati in seguito alla vulnerabilità del software MOVEit. Il gruppo CL0P è riuscito ad accedere inizialmente anche mediante l'utilizzo di altre tecniche, tra cui il phishing, e continua ad eseguire un modello RaaS (Ransomware-as-a-Service). Recentemente, il gruppo ha evoluto la sua tattica utilizzando la strategia della quadrupla estorsione sugli obiettivi presi di mira, come le istituzioni finanziarie. Oltre alle tecniche presenti nella tripla estorsione, la quadrupla estorsione include l'invio di messaggi volti a molestare partner aziendali, dipendenti, clienti, alti dirigenti e utenti dei social media per informarli che le loro organizzazioni hanno subito un attacco. Questa tattica ha portato ad un aumento del costo medio di un attacco ransomware.

Tra gli altri criminali hacktivisti che prendono di mira istituzioni finanziarie, ma non sono classificati come gruppi di ransomware, figurano Anonymous Sudan, KillNet e NoName057(16). Si tratta di gruppi tutti noti per le loro attività correlate alla guerra tra Russia e Ucraina. In particolare, il gruppo Anonymous Sudan ha dichiarato di aver partecipato anche agli attacchi informatici sferrati in risposta al conflitto tra Israele e Hamas. L'anno scorso, questi gruppi, oltre ad altri gruppi di criminali, sfruttando il caos provocato dalla guerra tra Russia e Ucraina, hanno rivolto la loro attenzione ad infrastrutture bancarie critiche.

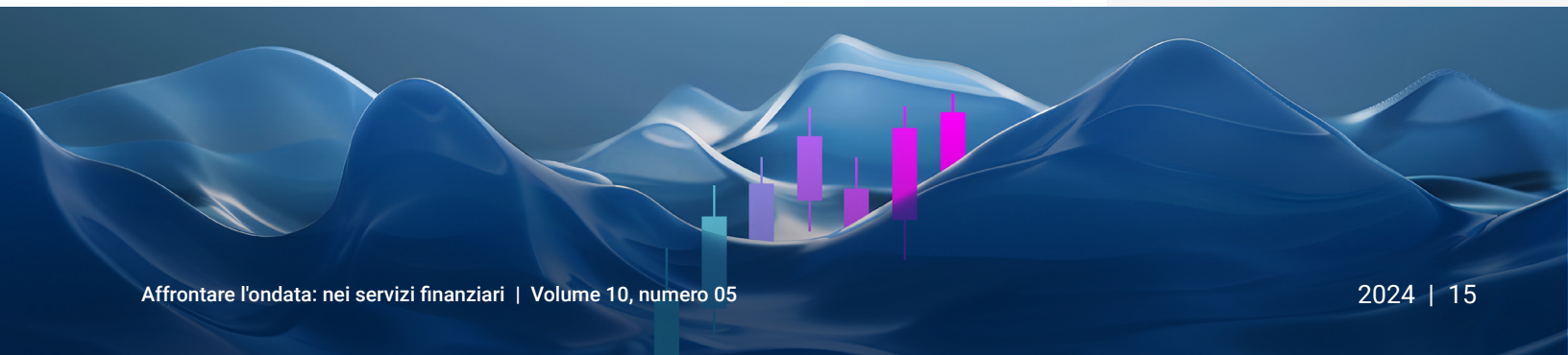
Esistono molti altri criminali prolifici che non sono classificati come gruppi di ransomware, ma che sono noti per aver preso di mira il settore dei servizi finanziari, come il gruppo Lazarus, MoneyTaker, Carbanak/FIN7, Cobalt e APT41.

Considerando le continue minacce poste da questi criminali, è fondamentale per le istituzioni finanziarie conoscere l'attuale panorama delle minacce e comprendere meglio le loro motivazioni e le tecniche utilizzate per sviluppare strategie di difesa più efficaci. Consultare la nostra sezione sulla mitigazione più avanti in questo rapporto per informazioni sulle misure di protezione consigliate.

La recente epidemia di hacktivismo DDoS in Medio Oriente che ha colpito le istituzioni finanziarie

Il settore dei servizi finanziari in Medio Oriente, recentemente, è stato caratterizzato da un'impennata di attacchi DDoS protratti e sofisticati, che sono stati favoriti dalle tensioni geopolitiche. Questa tendenza si è rivelata prevalente nell'area EMEA (Europa, Medio Oriente e Africa) ed è indicativa della crescente minaccia degli attacchi DDoS sferrati sulla base di motivazioni politiche contro le istituzioni finanziarie.

Un esempio significativo di questa tendenza si è verificato all'inizio di quest'anno quando BlackMeta (anche noto come DarkMeta), un gruppo di hacktivisti filopalestinesi, ha lanciato un attacco DDoS al livello 7, durato 6 giorni, contro un'istituzione finanziaria negli Emirati Arabi Uniti (UAE). L'attacco è stato facilitato da InfraShutdown, un servizio DDoS-for-hire, che ha evidenziato quanto sia sempre più facile accedere a questi strumenti di attacco. Il gruppo BlackMeta, attivo da novembre 2023, tradizionalmente prende di mira varie organizzazioni in Israele, nell'UAE e negli Stati Uniti.



L'attacco sferrato contro un'istituzione finanziaria nell'UAE è stato significativo sia per durata che per intensità: si è protratto per 100 ore circa, con ondate di richieste web di durata compresa tra 4 e 20 ore e una media di 4,5 milioni di richieste al secondo. La banca è rimasta sotto attacco per il 70% del tempo, il che ha influito notevolmente sui suoi servizi. La campagna di attacchi subiti dalla banca ad opera del gruppo BlackMeta ha fatto parte di un'iniziativa più ampia volta a protestare contro le ingiustizie avvertite nei confronti dei palestinesi e dei musulmani, mostrando tattiche simili a quelle utilizzate dal gruppo Anonymous Sudan.

Fortunatamente, gli sforzi di mitigazione dell'istituzione finanziaria hanno impedito il verificarsi di interruzioni più significative, ma questo incidente sottolinea la crescente tendenza da parte dei criminali di sferrare attacchi informatici sulla base di motivazioni politiche. Inoltre, evidenzia la disponibilità sempre maggiore di servizi DDoS-for-hire, che rendono più semplice per i gruppi di hacktivisti sferrare attacchi su larga scala. Questa nuova tendenza sottolinea anche la necessità di adottare solide misure di cybersicurezza per proteggersi da minacce persistenti e massicce.

Un altro recente attacco DDoS, che si sospetta sia stato sferrato sulla base di motivazioni politiche, si è verificato il 15 luglio 2024 e ha preso di mira una delle principali società di servizi finanziari in Israele. Questo imponente attacco, che è stato originato da una botnet distribuita a livello globale, è durato quasi 24 ore arrivando ad un picco di 798 Gbps. Akamai è riuscita a mitigare questo attacco DDoS ai livelli 3 e 4 che ha incluso vari vettori, come gli attacchi di riflessione DNS e UDP flood.

Durante questo attacco, Akamai ha bloccato circa 389 terabyte di traffico dannoso in una fase intensa di tre ore, raggiungendo un totale di traffico bloccato pari a circa 419 terabyte per l'intera durata dell'attacco. Il verificarsi di altre interruzioni affrontate dalle istituzioni finanziarie israeliane lo stesso giorno fa pensare ad un attacco coordinato, il che evidenzia ulteriormente la crescente minaccia posta da avanzati attacchi DDoS.

È importante notare che questo criminale esperto aveva già preso di mira gli stessi servizi finanziari 27 volte nei 90 giorni precedenti. Il cliente è stato ripetutamente colpito da attacchi DDoS a partire dal 4° trimestre 2023 in concomitanza con lo sfociare della guerra tra Israele e Hamas. Il gruppo interno di Akamai che si occupa dell'intelligence degli attacchi DDoS segnala che istituzioni e aziende in Israele hanno subito un numero senza precedenti di attacchi DDoS nel 2024. Questa campagna protratta e aggressiva evidenzia il livello crescente di portata e intensità di queste minacce a indicare che i criminali stanno diventando più tenaci e ingegnosi.

Fidarsi delle cose comuni: l'abuso dei brand nei servizi finanziari

In seguito all'adozione di un approccio principalmente digitale nei servizi finanziari per migliorare le customer experience, l'efficienza operativa, l'innovazione, i ricavi complessivi e la visibilità, i criminali informatici stanno sfruttando la fiducia esistente tra le organizzazioni e i loro clienti tramite schemi di impersonificazione dei brand. La Figura 7 mostra esempi di siti fraudolenti che imitano quelli di note istituzioni finanziarie. Anche se il phishing e l'impersonificazione dei brand sono metodi usati comunemente, destano particolare preoccupazione il numero allarmante di siti fraudolenti e la rapidità con cui i criminali riescono a creare nuovi domini dopo aver messo fuori uso i loro siti originali. Questa rapida proliferazione pone una crescente minaccia inesorabile sul settore dei servizi finanziari.

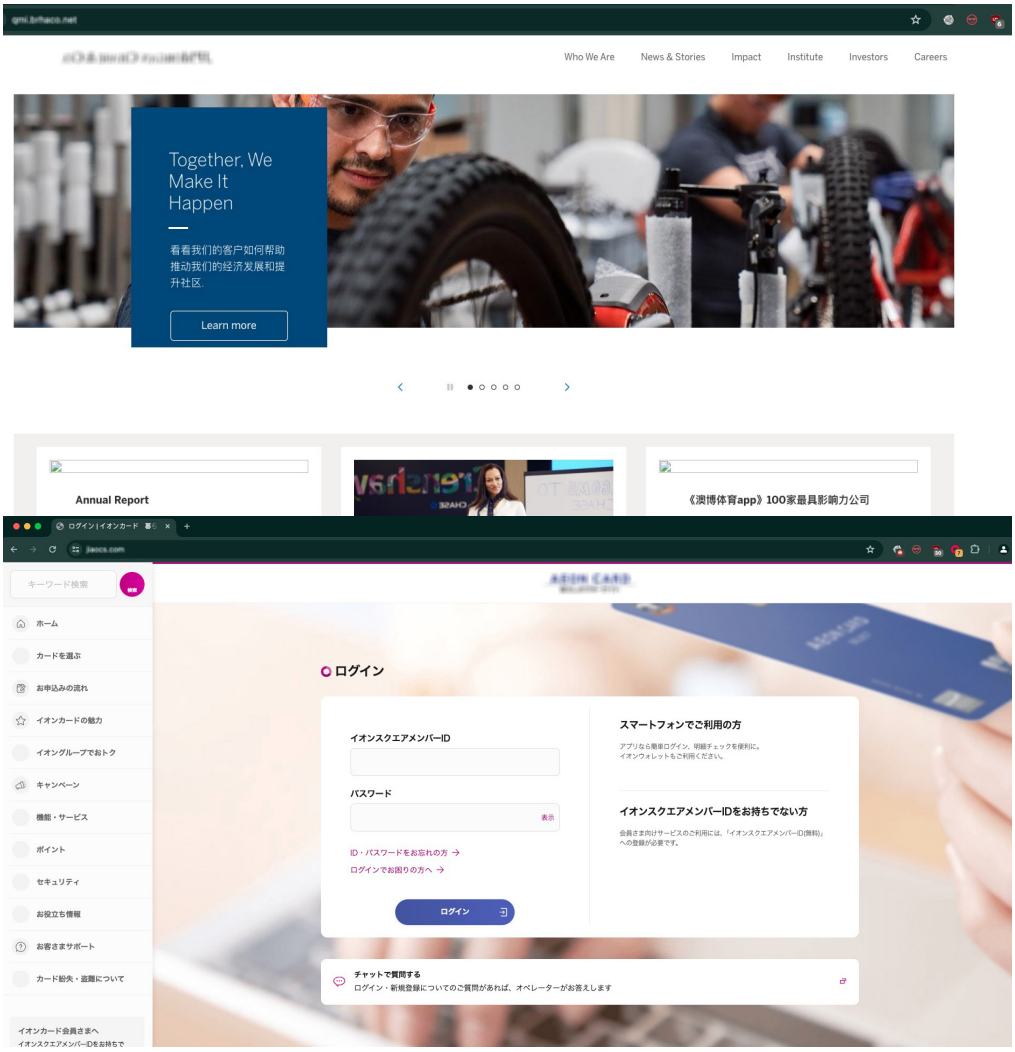


Figura 7. Esempi di siti di phishing fraudolenti che imitano quelli di note istituzioni finanziarie

Il panorama dell'abuso dei brand è stato notevolmente alterato dall'emergere degli attacchi di phishing come toolkit e piattaforme di servizio. Queste risorse hanno reso più semplice l'accesso per i criminali informatici, influendo drasticamente sulla portata e sull'entità degli attacchi di phishing contro i servizi finanziari e i loro clienti. Per chiarire la questione, il gruppo di lavoro anti-phishing ha registrato quasi 5 milioni di attacchi di phishing nel 2023, che è stato designato l'anno peggiore mai osservato per numero di phishing.

L'abuso dei brand può favorire un'escalation dei rischi, come il furto delle identità e l'abuso degli account. I criminali spesso vendono le informazioni dei clienti sul dark web o le utilizzano per assumere il controllo degli account. Dal punto di vista della sicurezza, è fondamentale intervenire tempestivamente negli attacchi contro i brand. Contrastando gli attacchi nelle fasi iniziali, è possibile impedire ai criminali di raccogliere le credenziali degli utenti per scopi illeciti.

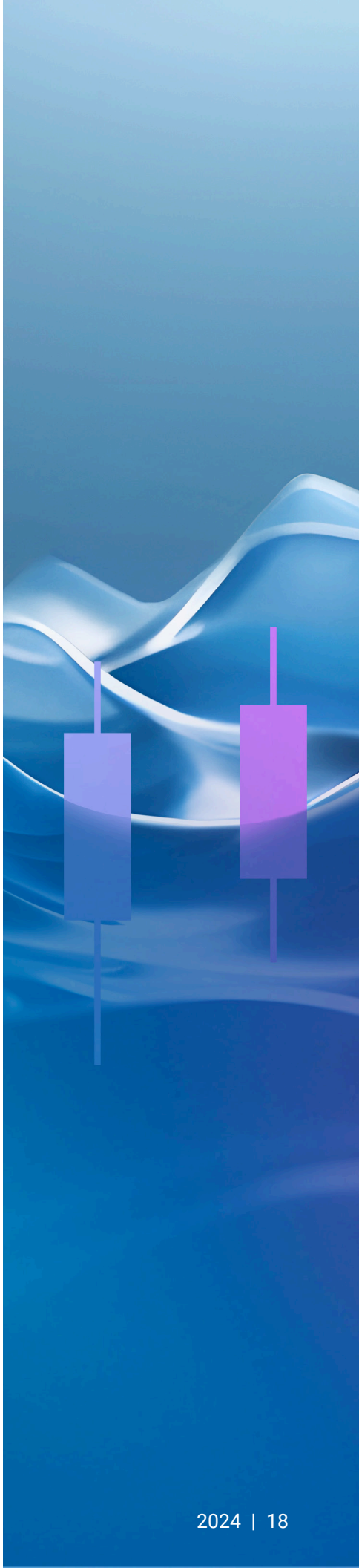
Le ramificazioni dell'abuso dei brand vanno oltre gli immediati problemi di sicurezza. Un'organizzazione può subire significative perdite finanziarie a causa dei danni alla reputazione, problemi di conformità e questioni legali e, persino, perdita di vendite per i prodotti contraffatti. Nell'odierno panorama digitale, il rilevamento tempestivo degli attacchi di impersonificazione dei brand è importantissimo per mantenere la fiducia dei clienti e la continuità aziendale.

Realtà o finzione? Uno sguardo ravvicinato agli attacchi di impersonificazione

I team addetti alla sicurezza devono affrontare la scoraggiante sfida di difendersi dai tentativi di abuso dei brand sulle varie piattaforme online, che rende arduo il compito di salvaguardare le risorse digitali poiché vi possono accedere sia utenti legittimi che criminali. I criminali spesso esfiltrano i contenuti di risorse rivolte al pubblico, come portali di banking online, per creare propri siti contraffatti e registrare domini con nomi errati per ingannare gli ignari utenti. Inoltre, i criminali informatici lanciano campagne che utilizzano e-mail di phishing, post di social media e altri canali digitali per attirare le potenziali vittime sulle loro app fittizie o sui loro siti dannosi.

In questo rapporto, abbiamo analizzato le attività di phishing e di impersonificazione dei brand osservate su domini attivi negli scorsi 12 mesi per fornire informazioni sulla prevalenza dei tentativi di impersonificazione dei brand nei vari settori, con un'attenzione particolare ai servizi finanziari. La visibilità completa e la soluzione proprietaria di Akamai consentono di:

- Tenere traccia del traffico instradato tramite i siti di phishing e di impersonificazione dei brand, inclusi i relativi marketplace
- Identificare il numero di domini dannosi attivi
- Valutare il livello di gravità dei domini dannosi



I servizi finanziari sono stati il settore che ha maggiormente subito attacchi di impersonificazione dei brand (36,25%) tra tutti i siti sospetti che ha monitorato Akamai (Figura 8). Questo risultato sottolinea, in particolare, quanto il settore dei servizi finanziari sia vulnerabile agli attacchi di abuso e impersonificazione dei brand, seguito, rispettivamente al secondo e al terzo posto, dai settori del commercio (26,41%) e dei servizi alle imprese (18,90%).

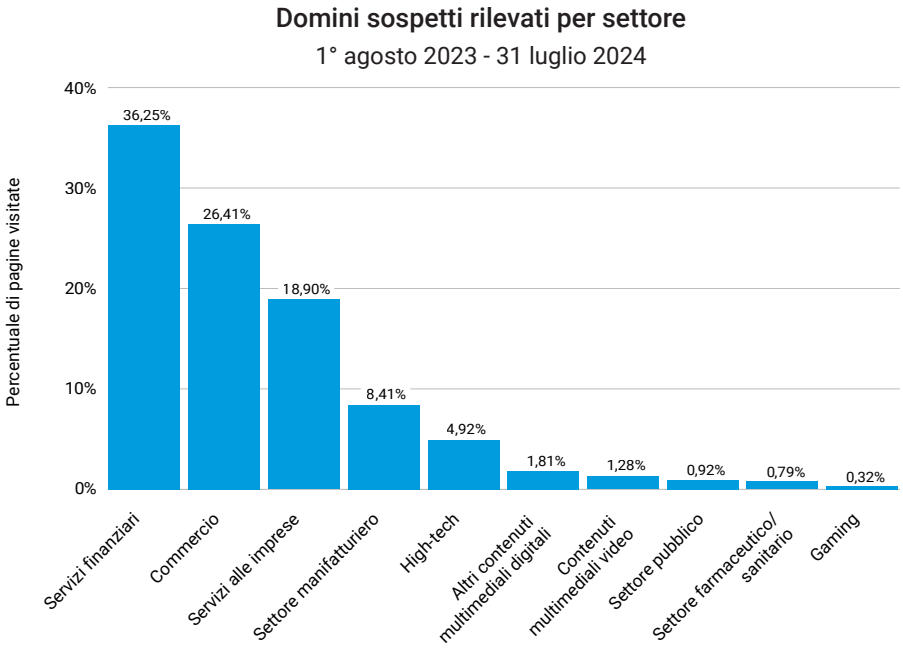


Figura 8. I servizi finanziari hanno registrato il 36,3% dei domini che hanno subito attacchi di phishing e/o impersonificazione dei brand

Il settore dei servizi finanziari è un obiettivo allettante per gli attacchi di impersonificazione dei brand a causa della vasta quantità di dati sensibili e preziosi di cui dispone, come le credenziali bancarie e le informazioni di identificazione personale (PII). I dati ottenuti da siti bancari contraffatti consentono ai criminali informatici di accedere facilmente ai conti desiderati per poi prosciugarli. Analogamente, i criminali possono ottenere altre informazioni finanziarie preziose come le credenziali per accedere a e-wallet e conti in criptovalute (che sul dark web costano dai 120 ai 400 dollari) allo scopo di trasferire le somme depositate o di vendere tali dati sui dark marketplace. L'elevato guadagno derivante da questi schemi rende i servizi finanziari l'obiettivo principale degli attacchi di abuso dei brand e phishing.

Analogamente, le organizzazioni commerciali sono diventate bersagli allettanti per l'abuso dei brand in seguito alla diffusione dell'e-commerce e dello shopping online, che presenta l'opportunità di sottrarre credenziali e altre informazioni personali. Le aziende manifatturiere e i fornitori di servizi di terze parti sono ugualmente vulnerabili all'abuso dei brand. Anche se la digitalizzazione migliora la crescita aziendale complessiva, è diventata un punto vulnerabile per molte organizzazioni, causando la proliferazione degli attacchi di impersonificazione dei brand e l'aumento dei tentativi di phishing.

L'elevato guadagno derivante dagli schemi [di impersonificazione dei brand] rende i servizi finanziari l'obiettivo principale degli attacchi di abuso dei brand e phishing.

Le organizzazioni devono rimanere all'erta e implementare misure di sicurezza in grado di proteggere sia i brand che i clienti in questo scenario digitale in continua evoluzione, tra cui il monitoraggio continuo per rilevare eventuali abusi dei brand, rapide procedure di rimozione dei siti fraudolenti e campagne di informazione per consentire ai clienti di riconoscere potenziali tentativi di impersonificazione. Dando priorità a queste iniziative, le organizzazioni possono salvaguardare meglio la loro reputazione e la fiducia dei loro clienti in uno scenario delle minacce sempre più complesso.

I servizi finanziari nel mirino degli attacchi di abuso dei brand

Per ottenere una visione olistica sull'impatto degli attacchi di impersonificazione dei brand e di phishing, abbiamo anche analizzato il numero di pagine visitate sui siti sospetti. Dai nostri risultati, è emerso che i siti che si spacciano per quelli di istituzioni finanziarie legittime hanno ricevuto il 30% delle visite, seguiti da quelli che si fingono siti di società commerciali con il 20% delle visite (Figura 9). Questi risultati posizionano in modo coerente i servizi finanziari e il commercio tra i settori più colpiti, sia per numero di richieste che di domini impersonificati. Questa coerenza evidenzia come questi settori vengano considerati gli obiettivi principali degli attacchi di abuso e impersonificazione dei brand e per un buon motivo.

I servizi finanziari comprendono una vasta gamma di obiettivi, dalle banche più importanti alle istituzioni di minori dimensioni con un numero ridotto di risorse di sicurezza, che sono tutti componenti ad alto rischio. Anche il commercio, un altro settore sottoposto ad una simile attenzione da parte degli enti di controllo della conformità (ad es., il Payment Card Industry Security Standards Council), si trova ad affrontare rischi significativi a causa delle preziose informazioni sui clienti di cui dispone.

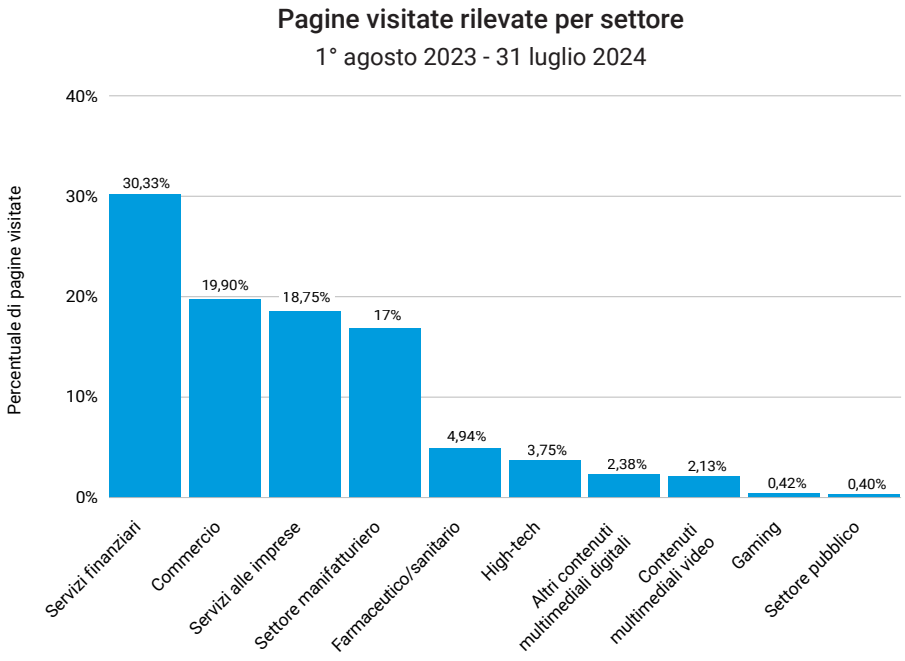


Figura 9. Più del 30% delle pagine visitate durante il periodo esaminato nel rapporto (agosto 2023 - luglio 2024) è da ricondurre a siti sospetti che si sono spacciati per siti legittimi di servizi finanziari

Un aspetto interessante che abbiamo osservato riguarda le differenze tra le posizioni in cui si sono collocati i tentativi di impersonificazione dei domini e il numero effettivo di pagine visitate per i vari settori. Ad esempio, l'high-tech si è posizionato tra i primi cinque settori per numero di domini impersonificati, ma scende al sesto posto per numero di pagine visitate. Analogamente, un minor numero di domini impersonificati si sono registrati nel settore farmaceutico/sanitario, ma si è verificato un numero maggiore di visite a questi domini.

Il phishing per ottenere le credenziali

L'abuso dei brand assume molte forme, inclusi siti clonati che replicano esattamente il logo e il design del sito legittimo di un'azienda, app fraudolente e profili falsi dei social media che imitano gli account aziendali ufficiali. Per comprendere la portata di questo problema, abbiamo analizzato le pagine contraffate suddividendole in varie categorie: impersonificazione dei brand, phishing, app non autorizzate, store falsi, strumenti di bypass dei paywall e store/profili falsi dei social media. È importante notare che il dominio di una sola organizzazione può rientrare in più classificazioni in base alle pagine che abbiamo monitorato.

Dalla nostra analisi, è emerso che il phishing colpisce i domini contraffatti che prendono di mira i servizi finanziari, rappresentando, in modo sconcertante, il 68% di tutte le istanze registrate (Figura 10). L'impersonificazione dei brand segue al secondo posto, rappresentando il 24% di tutti i domini registrati. Tra i siti più frequentati dagli utenti, quelli di phishing e di impersonificazione dei brand si collocano, rispettivamente, al primo e al secondo posto. Altre forme di abuso dei brand, come store/profili falsi dei social media, colpiscono meno le istituzioni finanziarie rispetto ad altri settori. Nonostante il minor numero di attacchi che prendono di mira le app non autorizzate, è importante notare che i criminali stanno adottando metodi sempre più creativi per ampliare la portata dei loro attacchi.

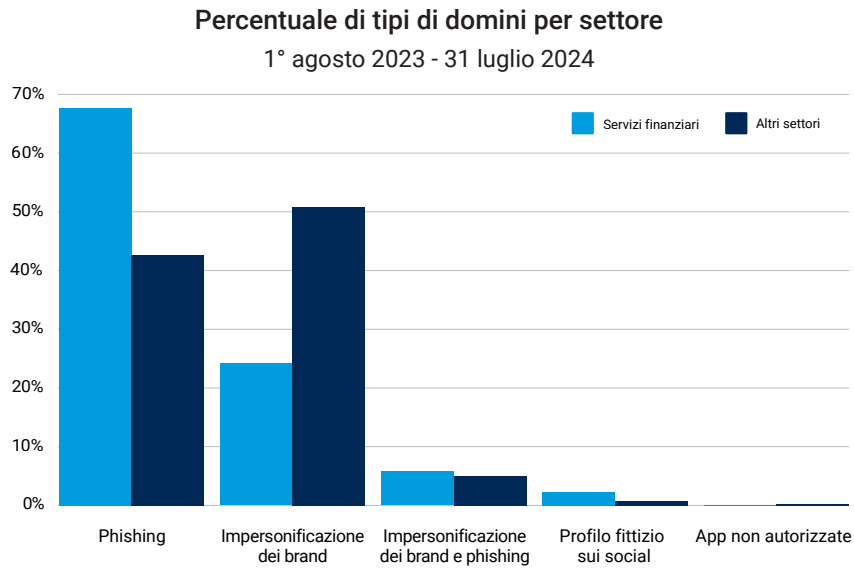


Figura 10. La maggior parte dei domini che abbiamo registrato per i servizi finanziari è rappresentata da siti di phishing, il cui numero supera addirittura il totale di tutti gli altri settori messi insieme

Le istituzioni finanziarie vengono considerate estremamente affidabili, il che le rende i principali obiettivi per i criminali che sfruttano questo livello di fiducia.

Nonostante la maggiore consapevolezza dei rischi posti dal phishing, l'elemento umano rimane una notevole falla nella sicurezza. Questo problema viene esacerbato dalle sofisticate tecniche usate dai criminali (per ulteriori informazioni, è possibile consultare la sezione L'anatomia dell'abuso dei brand), che rendono difficile individuare una pagina fittizia per chi non ha le competenze necessarie. Le istituzioni finanziarie vengono considerate estremamente affidabili, il che le rende i principali obiettivi per i criminali che sfruttano questo livello di fiducia. Impersonando queste istituzioni, i criminali inducono gli utenti a fornire consapevolmente le loro credenziali, sfruttando la reputazione dell'istituzione in questione per rendere le loro truffe più convincenti ed efficaci.

Per salvaguardare un'organizzazione e i suoi clienti, è fondamentale usare le tecnologie di sicurezza con funzionalità di monitoraggio dei brand per monitorare in modo proattivo eventuali utilizzi non autorizzati, sia che si tratti di un nome di dominio, un'app mobile o un messaggio e-mail, e, una volta identificati, condurre le operazioni necessarie per contrastare il traffico che potrebbe esporre i clienti ai pericoli (come il furto di dati) posti dagli attacchi di abuso dei brand e di phishing.

Case study: la crescente complessità degli attacchi di credential stuffing contro le istituzioni finanziarie

Una società di tecnofinanza negli Stati Uniti ha subito, per tutto il 2023 e il 2024, inesorabili attacchi di credential stuffing che hanno preso di mira una delle sue applicazioni rivolte ai clienti. L'entità di questi attacchi è sconcertante: in un periodo di 24 ore, Akamai ha rilevato più di 3.000 avvisi provenienti da diversi indirizzi IP che tentavano di infiltrarsi negli account presi di mira tramite credenziali rubate. Abbiamo osservato un indirizzo IP che, da solo, ha tentato almeno 115 combinazioni di nome utente e password. In totale, abbiamo registrato più 100.000 avvisi a luglio 2024.

Livello di rischio critico per i siti fraudolenti dei servizi finanziari

Le informazioni esclusive ricavate dalla nostra piattaforma edge globale insieme agli altri dati provenienti dall'intelligence sulle minacce di terze parti ci offrono un notevole vantaggio nel rilevare le impersonificazioni dei brand. Questo sistema completo ci serve per esaminare scrupolosamente e per classificare ogni dominio in base al suo punteggio di pericolosità.

Questo punteggio viene calcolato considerando tre fattori principali:

1. **La certezza**: la certezza di saper riconoscere che un evento è un tentativo di phishing
2. **La gravità**: il livello di rischio (critico, alto, medio o basso) associato ad un evento
3. **La frequenza**: il numero di sessioni/eventi associati al sito in un determinato periodo di tempo

Il nostro sistema di assegnazione dei punteggi bilancia questi tre fattori principali (certezza, gravità e frequenza), combinando i relativi valori per generare un punteggio completo per ogni dominio sospetto, fino ad un massimo di 99, in modo da garantire una valutazione olistica delle potenziali minacce.

Dalla nostra ultima analisi, è emerso che il settore dei servizi finanziari ha fatto registrare un preoccupante punteggio medio di pericolosità pari a 85 a indicare i notevoli rischi che il settore continua ad affrontare (Figura 11). Questo punteggio mette le istituzioni finanziarie alla portata dei criminali informatici, che prendono incessantemente di mira i loro vasti archivi di dati sensibili.

Punteggi di pericolosità per settore

Settore	Punteggio medio di pericolosità	Settore	Punteggio medio di pericolosità
Pubblica amministrazione	**95**	Gaming	**65**
Servizi finanziari	**85**	Settore manifatturiero	**64**
Servizi alle imprese	**85**	Altri contenuti multimediali digitali	**62**
Settore farmaceutico/sanitario	**85**	Commercio	**61**
Contenuti multimediali video	**71**	High-tech	**60**

Figura 11. Il nostro calcolo dei punteggi medi di pericolosità mostra un valore allarmante per i servizi finanziari

Mentre il settore pubblico ha registrato il punteggio medio di pericolosità più alto, probabilmente a causa dell'elevata quantità di informazioni sensibili e delle limitate risorse di sicurezza di cui dispone, i servizi finanziari rimangono un bersaglio ugualmente allettante in quanto i criminali sono attirati dalla possibilità di ottenere un enorme ritorno economico. Anche i servizi alle imprese e il settore farmaceutico/sanitario hanno fatto registrare punteggi simili a indicare che i criminali informatici stanno diversificando i loro obiettivi. Tuttavia, le istituzioni finanziarie rimangono un obiettivo privilegiato a causa della natura critica dei loro dati.

Questo elevato livello di pericolosità richiede un'azione immediata per rafforzare i sistemi di difesa e per mitigare le minacce in continua evoluzione prima che possano condurre a notevoli perdite finanziarie e danni alla reputazione.

L'anatomia dell'abuso dei brand

L'entità delle campagne di phishing e impersonificazione è resa ancora maggiore dalla presenza dei toolkit di phishing.

Il successo delle frodi e dell'abuso dei brand dipende in larga misura dal potere dei brand come esca di social engineering. I criminali sfruttano il senso di familiarità e la fiducia dei clienti nei confronti dei brand più famosi, progettando siti fittizi che riproducono fedelmente quelli legittimi. In alcuni casi, i truffatori copiano persino esattamente il codice, rendendo questi siti illegittimi praticamente identici a quelli reali. Con la diffusione degli strumenti di AI generativa, che aiutano i truffatori ad eliminare gli errori di ortografia e grammatica che possono risultare segni rivelatori di una minaccia, è diventato ancora più difficile per i consumatori distinguere i siti autentici da quelli fittizi.

L'entità delle campagne di phishing e impersonificazione è resa ancora maggiore dalla presenza dei toolkit di phishing. Ad un costo irrisorio di 50 dollari, i criminali possono acquistare toolkit di phishing con cui poter creare siti di phishing convincenti. L'impresa dei criminali informatici che prevede lo sviluppo, la creazione e la vendita di toolkit di phishing rende molto più semplice condurre campagne di phishing e impersonificazione. Kr3pto e 16Shop sono due esempi dei toolkit di phishing più comuni. Kr3pto ha preso di mira alcune banche nel Regno Unito bypassando l'autenticazione a due fattori, mentre 16Shop ha colpito principalmente brand importanti come PayPal e Amazon, solo per citarne alcuni. Ad agosto 2023, un'operazione internazionale condotta dalle forze dell'ordine si è conclusa con l'arresto dei creatori di 16Shop. Questi esempi evidenziano la crescente complessità degli attacchi di phishing e gli sforzi congiunti intrapresi per combattere il crimine informatico.

Sottovalutato ma efficace: il combosquatting

Un altro importante aspetto dell'abuso dei brand è l'utilizzo di nomi di dominio molto simili a quelli dei siti legittimi. Di solito, i criminali registrano i loro domini dopo aver acquistato o costruito il proprio sito di phishing. Ed è a questo punto che svolgono un ruolo cruciale tecniche di comprovata validità come il cybersquatting e le sue numerose varianti. Una tattica usata comunemente è il typosquatting, in cui i criminali registrano un dominio con il nome di un'azienda contenente un piccolo errore ortografico (ad es., acamai[.]com), sperando che l'utente lo digiti in questo modo. Un altro metodo, il combosquatting, richiede l'aggiunta di altre parole, come "supporto", "login" o "aiuto", al nome del dominio. Questa tattica sfrutta i micrositi che si trovano spesso nei siti aziendali legittimi.

Secondo una ricerca condotta da Akamai, nonostante sia una tattica poco segnalata, il combosquatting (che consiste nell'aggiunta di una parola chiave) supera il typosquatting (che consiste nell'aggiunta, nella rimozione o nella sostituzione di un carattere) per numero di domini attivi. È interessante notare che "com" è risultata una delle parole chiavi più aggiunte nei siti fraudolenti.

Il meccanismo di distribuzione

I siti di phishing e contraffatti vengono distribuiti e messi in circolazione tramite vari meccanismi, tra cui più comunemente mediante i messaggi e-mail, che sembrano convincenti perché utilizzano un logo legittimo e contengono comunicazioni urgenti, come richieste di aggiornamento dei dati di un conto. Tuttavia, l'abuso dei brand non è limitato ai siti web e alle e-mail: i criminali diffondono le minacce anche tramite i social media, espandendo così ulteriormente la loro portata e le tattiche utilizzate per ingannare gli utenti.

Collegamenti nascosti in bella vista

Esistono altre tattiche osservate in rete che rendono più difficile identificare un sito di impersonificazione da parte dei consumatori e che possono incrementare il successo di questi attacchi. Ad esempio, l'uso di URL abbreviati, codici QR, hyperlink di immagini e collegamenti a testi negli SMS nascondono i link dannosi. A differenza della posta elettronica che offre filtri anti-spam per proteggere da questo abuso, gli SMS inviati a scopi dannosi probabilmente non vengono bloccati e hanno più possibilità di venire letti o aperti.

Esistono altre tattiche osservate in rete che rendono più difficile identificare un sito di impersonificazione da parte dei consumatori e che possono incrementare il successo di questi attacchi.

Gli attacchi di phishing e impersonificazione dei brand nei servizi finanziari in specifiche aree geografiche

L'abuso dei brand interessa le organizzazioni e i consumatori di tutto il mondo, tuttavia, alcune aree geografiche mostrano una vulnerabilità maggiore alle frodi e agli abusi a causa della concentrazione di traffico verso i siti di phishing e impersonificazione dei brand. Dalla nostra analisi, è emerso che l'area EMEA ha registrato la maggiore quantità di traffico verso i siti di phishing e impersonificazione negli ultimi 12 mesi, superando persino quella del Nord America (Figura 12), sia nei servizi finanziari che in altri settori.

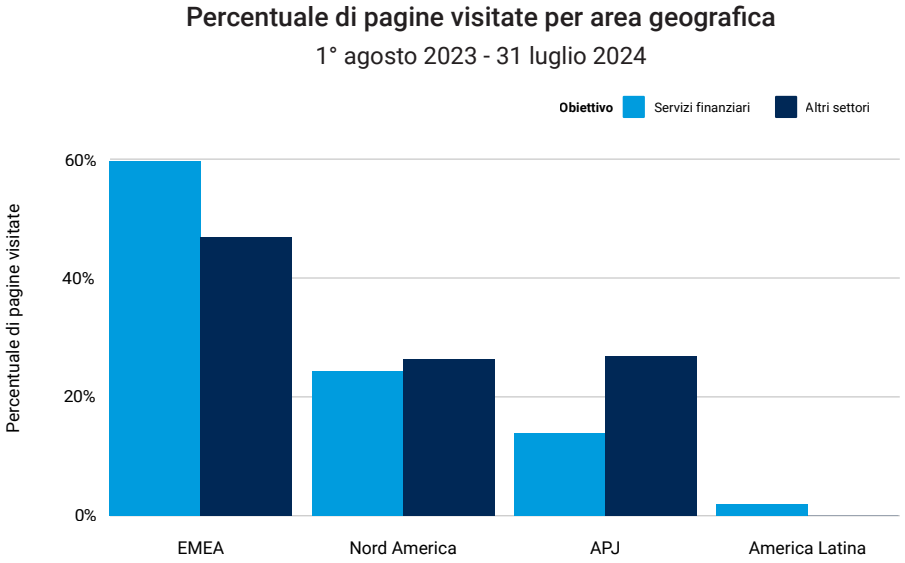
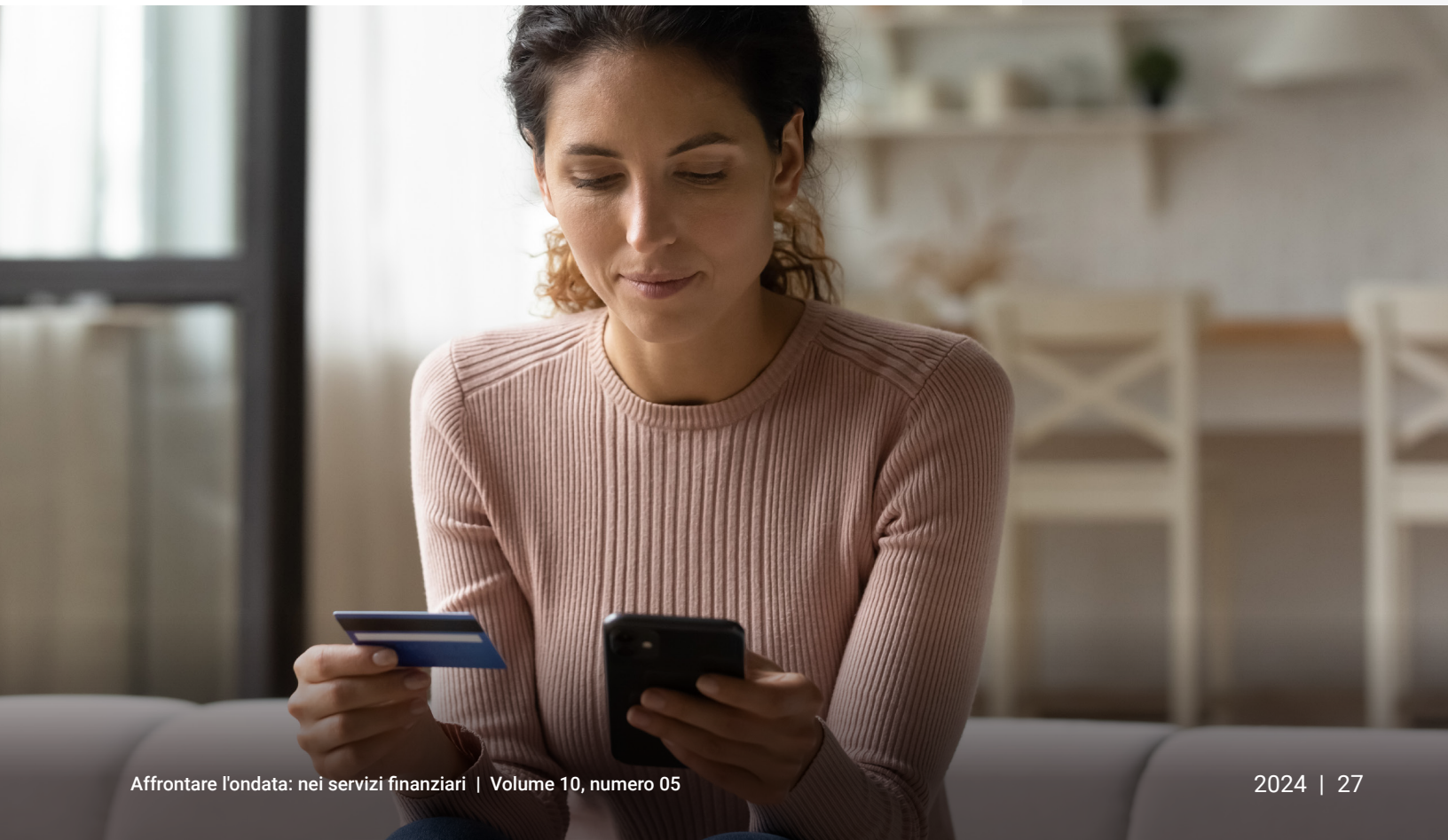


Figura 12. L'EMEA ha superato il Nord America imponendosi come l'area geografica più colpita dal phishing e dall'abuso dei brand nei servizi finanziari

Anche se l'America Latina e l'area APJ (Asia-Pacifico e Giappone) hanno registrato numeri relativamente ridotti di pagine visitate, questo dato non indica che siano state meno colpite di altre aree geografiche. Anzi, questi risultati probabilmente riflettono la concentrazione di brand globali con un elevato numero di clienti in Nord America e nell'EMEA, il che aumenta il numero di potenziali vittime per i criminali. Possiamo attribuire questi risultati anche all'emergere dei toolkit di phishing, come V3B, che ha specificatamente preso di mira alcune banche europee a partire dal 2023.

Anche se l'EMEA supera la maggior parte delle aree geografiche per numero di domini sospetti e di pagine visitate, l'APJ fa registrare il punteggio medio di pericolosità più alto: 97. L'America Latina, nonostante il numero di visite ai siti più basso, riceve un sorprendente punteggio medio di pericolosità pari a 94 a indicare che i consumatori sia in America Latina che nell'APJ sono maggiormente a rischio di subire il furto delle loro informazioni bancarie e di altri dati sensibili durante la visita di siti web.

Numerosi fattori contribuiscono all'aumento dei pericoli posti dall'abuso dei brand contro i servizi finanziari nell'APJ, dove, innanzitutto, la maggior parte delle istituzioni finanziarie è altamente digitalizzata: praticamente ogni servizio offerto può essere eseguito online senza neanche recarsi in una sede fisica. La velocità di penetrazione di Internet e dell'adozione digitale nell'APJ è una delle più alte a livello globale, pertanto quest'area geografica è diventata un bersaglio allettante per i criminali informatici. In secondo luogo, quest'area geografica comprende alcuni dei paesi con i social media più attivi al mondo. Inoltre, le istituzioni finanziarie hanno aumentato l'engagement dei clienti tramite queste piattaforme per competere per le quote di mercato e aumentare la fedeltà dei clienti. Il diffuso utilizzo dei social media e delle app di messaggistica nell'area APJ fornisce ai criminali informatici ulteriori vettori per sferrare attacchi di phishing e impersonificazione, spesso abusando della fiducia riposta dagli utenti in queste piattaforme.



L'evoluzione della conformità: in che modo le normative in materia di cybersicurezza stanno trasformando le istituzioni finanziarie

Quando gli fu chiesto perché avesse scelto proprio le banche per i suoi colpi, il celebre rapinatore Willie Sutton rispose: "Perché è lì che stanno i soldi". La dichiarazione di Sutton, ovviamente, si può applicare facilmente agli attacchi informatici sferrati ai giorni nostri contro le istituzioni finanziarie. La motivazione del guadagno economico, tuttavia, è solo una parte della storia. Le istituzioni finanziarie sono sempre più sotto il fuoco di criminali animati da motivazioni politiche, nonché da ragioni strategiche dettate dalle situazioni geopolitiche. Queste motivazioni, insieme con il concetto del colpire dove "stanno i soldi", creano una bufera perfetta per le istituzioni finanziarie che sono in cima alla classifica dei settori maggiormente presi di mira.

Questo dato non deve sorprenderci. Il settore finanziario ha sempre giocato un ruolo critico e centrale nella nostra società ed è da sempre ampiamente regolamentato. Anche se le normative che hanno regolato le istituzioni finanziarie in passato si sono focalizzate sulla protezione dei consumatori nei loro rapporti con tali istituzioni, gli enti di controllo ora cercano di applicare regolamenti fondamentali in materia di sicurezza e resilienza alle istituzioni finanziarie e alle società di servizi. Questa nuova tendenza include requisiti da seguire non solo per le istituzioni finanziarie, ma anche per i loro fornitori ICT (Information and Communication Technology).

Sono numerosi gli esempi di normative sulla cybersicurezza e sulla resilienza operativa. Nell'Unione europea, il DORA (Digital Operational Resilience Act) obbliga gli enti finanziari e i loro fornitori ad adottare una solida struttura di gestione dei rischi ICT e a condurre l'esecuzione di test e la segnalazione degli incidenti in modo regolare. Negli Stati Uniti, la SEC (Securities and Exchange Commission) ha introdotto normative sugli aspetti materiali dei rischi informatici, richiedendo alle società pubbliche, incluse le istituzioni finanziarie, di divulgare gli incidenti informatici che potrebbero influire materialmente sulle loro attività aziendali. In Australia, l'APRA (Australian Prudential Regulation Authority) ha stabilito appositi standard che richiedono agli enti di mantenere le funzionalità sulla sicurezza delle informazioni commisurate alle dimensioni e all'entità delle minacce contro le loro risorse informative (normativa CPS 234). Questi esempi illustrano un andamento globale che tende a migliorare la cybersicurezza e la resilienza operativa dei settori finanziari per proteggersi dai rischi in continua evoluzione e per garantire la stabilità finanziaria.

Considerando queste normative, per le istituzioni finanziarie è d'obbligo effettuare controlli di due diligence durante l'acquisto di servizi per la sicurezza e ICT allo scopo di garantire che i fornitori rispettino questi standard sempre più rigorosi. Le istituzioni finanziarie devono scegliere fornitori in grado non solo di offrire un servizio resiliente, ma anche di assorbire le normative rilevanti, fornire la visibilità necessaria per identificare e mitigare le minacce in continua evoluzione e aiutare ad applicare tali informazioni alle attività in corso.

La visibilità è fondamentale perché non potete proteggere ciò che non sapete di avere (o ciò a cui siete connessi) né potete difendervi da una minaccia se non sapete che c'è. Alcuni servizi come la piattaforma Akamai Guardicore forniscono non solo la protezione dagli attacchi, ma aiutano anche i clienti a capire i flussi di dati, ad identificare le anomalie e a segmentare correttamente le risorse di rete per mitigare le minacce. Analogamente, i suoi servizi di sicurezza delle API sono progettati per identificare il traffico delle API in modo da aiutare con le API ombra, nonché riconoscere i potenziali attacchi tramite le API.

Le banche devono forse aggiungere un livello di visibilità alla tradizionale triade (riservatezza, integrità e disponibilità) per riflettere questa nuova tendenza (visibilità, riservatezza, integrità e disponibilità).

James Casey
Vice President, Chief Privacy Officer,
Akamai

Migliorare i sistemi di difesa con la sicurezza Zero Trust

La fiducia è la base su cui si fonda la reputazione delle istituzioni finanziarie. Tuttavia, quando si tratta di salvaguardare ambienti complessi e dati riservati, la fiducia può diventare facilmente una grossa responsabilità. I criminali, spesso, sfruttano la fiducia implicita in moltissimi modi, tra cui:

- Attacchi di phishing per impersonificare singoli utenti all'interno dell'organizzazione
- Attacchi per sfruttare le vulnerabilità della sicurezza nei fornitori di terze parti allo scopo di accedere a obiettivi di valore elevato
- Minacce interne che abusano degli accessi per scopi illeciti

La crescente complessità degli attacchi ha reso inadeguato il tradizionale metodo di sicurezza perimetrale, che considera affidabile tutto il traffico proveniente dall'interno dell'azienda. Poiché la posta in gioco nei servizi finanziari è alta, mantenere un sistema di sicurezza resiliente è fondamentale. Ed è qui che diventa imprescindibile il modello Zero Trust. Questo approccio alla sicurezza si basa sul principio secondo cui qualsiasi richiesta di connessione, utente o dispositivo possa costituire un potenziale pericolo, mettendo, di conseguenza, in atto verifiche continue ed eliminando il concetto di fiducia implicita, ossia negando automaticamente l'accesso alle risorse, a meno che il richiedente non sia stato autenticato e autorizzato.

Il modello Zero Trust migliora la conformità ai requisiti normativi in continua evoluzione per le istituzioni finanziarie proteggendo i sistemi che trattano dati regolamentati e consentendo, pertanto, alle organizzazioni di evitare di incorrere in sanzioni in caso di mancato superamento degli audit. Questo modello fornisce ulteriori controlli per i sistemi tradizionali, offrendo la visibilità necessaria per rilevare gli utenti non autorizzati che tentano di accedere alle applicazioni critiche.

Il modello Zero Trust restringe il traffico est-ovest limitando l'accesso alla rete solo ai sistemi critici e impedendo il movimento laterale di minacce come il ransomware. Questa strategia di contenimento protegge i dati e le risorse essenziali isolando i sistemi infetti. Poiché il numero di attacchi ransomware contro i servizi finanziari è aumentato notevolmente, non si rimarcherà mai abbastanza l'importanza del modello Zero Trust nella protezione delle informazioni sensibili. Con la sua visibilità approfondita, il modello Zero Trust consente di rilevare e neutralizzare le minacce negli ambienti complessi, che sono operazioni cruciali per impedire la diffusione del ransomware e proteggere le risorse critiche.

Un altro importante vantaggio offerto dal modello Zero Trust consiste nella sua capacità di proteggere i flussi di dati tra le applicazioni, che è fondamentale per distribuire le applicazioni nel cloud in modo sicuro, non solo per facilitare la modernizzazione, ma anche per garantire la protezione delle informazioni riservate in un panorama delle minacce sempre nuovo, consentendo alle istituzioni finanziarie di innovarsi senza compromettere la sicurezza. L'implementazione di un sistema Zero Trust migliora il livello di sicurezza e protegge un'istituzione dalle minacce in continua evoluzione anche per il futuro.

La segmentazione va bene. La microsegmentazione è ancora meglio.

La segmentazione è un approccio architetturale che divide una rete in segmenti più piccoli per migliorare le performance e la sicurezza. La microsegmentazione è una tecnica di sicurezza che vi consente di dividere in modo logico una rete in segmenti separati fino al livello dei singoli carichi di lavoro. È possibile quindi definire i controlli di sicurezza e la delivery di servizi per ogni singolo segmento.

La microsegmentazione è anche la pietra miliare del modello Zero Trust. In un recente rapporto stilato da Akamai, i responsabili della cybersicurezza nei servizi finanziari hanno citato l'innovazione del modello Zero Trust come il fattore trainante che più frequentemente favorisce l'implementazione di un progetto di segmentazione. In effetti, quasi tutti i responsabili che hanno adottato la segmentazione stanno implementando o hanno già implementato un sistema di sicurezza Zero Trust (99%), anche se meno della metà di essi (47%) segnala che il proprio sistema Zero Trust è finalizzato e definito e, pertanto, può essere considerato avanzato.

La microsegmentazione è compatibile con i sistemi esistenti e viene implementata più rapidamente rispetto ai metodi tradizionali, come i firewall. Questo approccio velocizza la risposta dei ransomware anche di 13 ore e semplifica la gestione di tutti gli ambienti IT, aiutando, al contempo, a rispondere alle esigenze di conformità tramite un accurato controllo dei dati.

Un esempio reale mostra l'impatto della microsegmentazione moderna: in un progetto, il tempo di implementazione è stato ridotto da 2 anni a 6 settimane, è stato usato un solo tecnico e i costi sono diminuiti dell'85%. Questo esempio mostra come la microsegmentazione può far risparmiare tempo e denaro alle organizzazioni. I direttori dei reparti IT dovrebbero confrontare questi risultati con il tempo di implementazione e i costi per la sicurezza attualmente richiesti dalle loro organizzazioni.

Per rafforzare il proprio sistema di cybersicurezza, le istituzioni finanziarie devono dare priorità all'implementazione di avanzate strategie di segmentazione. I CISO dovrebbero impegnarsi nell'intento di allineare le misure di sicurezza agli standard di settore in continua evoluzione, integrando la microsegmentazione come una pietra miliare di una solida architettura Zero Trust. I direttori dei reparti IT devono stabilire una cadenza per l'esecuzione di regolari verifiche di sicurezza e aggiornamenti della strategia in modo da garantire che i propri sistemi di difesa rimangano resilienti alle minacce informatiche più complesse.

Questo approccio proattivo non solo aiuta a mitigare le attuali vulnerabilità, ma posiziona anche le organizzazioni in modo da contrastare efficacemente le nuove sfide della cybersicurezza. Adottando queste misure, le istituzioni finanziarie creano un sistema completo di sicurezza in grado di affrontare i problemi immediati e la gestione dei rischi a lungo termine.

[La microsegmentazione] non solo aiuta a mitigare le attuali vulnerabilità, ma posiziona anche le organizzazioni in modo da contrastare efficacemente le nuove sfide della cybersicurezza.

Akamai

Mitigazione

Quando si tratta di proteggere le istituzioni finanziarie da varie minacce informatiche, è necessario implementare un approccio multiforme. Andiamo ora a scoprire le principali strategie di mitigazione degli attacchi di phishing, impersonificazione dei brand, DDoS e ransomware.

Protezione dagli attacchi di phishing e impersonificazione dei brand

Per salvaguardare le istituzioni dagli attacchi di phishing e impersonificazione dei brand, consideriamo l'utilizzo di servizi di protezione dei brand di terze parti per rilevare e rimuovere rapidamente i contenuti fraudolenti. Inoltre, è importante fornire informazioni al riguardo a dipendenti e clienti, condurre regolari corsi di formazione sulla sicurezza consapevole per consentire al personale di riconoscere i tentativi di phishing e impersonificazione dei brand, fornire una guida chiara su come identificare le comunicazioni inviate legittimamente da un'istituzione e stabilire un piano di risposta rapido per i tentativi di impersonificazione, incluse le operazioni necessarie per informare partner e clienti sui furti di identità.

Inoltre, è consigliabile implementare queste tecniche di protezione:

- Registrare nomi di domini simili per evitare il typosquatting e utilizzare servizi di monitoraggio dei domini per rilevare i domini clonati.
- Rafforzare i protocolli di autenticazione utilizzando password complesse e univoche, oltre a gestori di password, e implementare una solida autenticazione multifattore (MFA) per tutti gli account e i sistemi.
- Distribuire protocolli di autenticazione e-mail, come SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting and Conformance) per evitare lo spoofing della posta elettronica. Utilizzare soluzioni anti-phishing e avanzati filtri e-mail per rilevare e bloccare le e-mail inviate a scopi dannosi.
- Proteggere i siti web e i canali digitali richiedendo i certificati SSL, implementando i protocolli HTTPS e utilizzando strumenti antifrode per rilevare attività sospette su siti web e app mobili.
- Salvaguardare i canali di comunicazione fornendo portali sicuri e implementando la crittografia dei messaggi per la corrispondenza riservata.

Protezione dagli attacchi DDoS

La protezione delle istituzioni finanziarie dagli attacchi DDoS richiede una strategia di difesa multilivello, che consiste nell'implementare strategie proattive, come l'utilizzo di prodotti specializzati per il rilevamento, la mitigazione e la protezione dagli attacchi DDoS, la configurazione della limitazione della velocità e la memorizzazione nella cache di contenuti su una CDN. Inoltre, è necessario tenersi informati sulle misure di sicurezza come la gestione delle patch, i piani di risposta agli incidenti, i controlli di mitigazione per indirizzi IP vulnerabili agli attacchi DDoS e sottoreti critiche, policy per il controllo degli accessi, segmentazione di rete e firewall Implementare strategie proattive, come la configurazione della limitazione della velocità, il caching dei contenuti su una CDN e l'utilizzo di prodotti specializzati per il rilevamento, la mitigazione e la protezione DDoS.

Per salvaguardare l'infrastruttura DNS, è fondamentale monitorare e analizzare continuamente il traffico DNS in entrata e scegliere una piattaforma ibrida anziché un firewall DNS tradizionale. Conoscere le tattiche, le tecniche e le procedure utilizzate dai criminali aiuta a proteggersi meglio dagli attacchi DDoS.

Protezione dai ransomware

Come citato in precedenza in questo rapporto, implementare il modello Zero Trust con la segmentazione di rete, specialmente la microsegmentazione, è fondamentale per limitare la diffusione del ransomware all'interno delle istituzioni finanziarie. L'adozione di solide misure di cybersicurezza, come questa, aiuterà a combattere le avanzate tecniche utilizzate dagli autori degli attacchi ransomware. Inoltre, è consigliabile stare all'erta e utilizzare il framework MITRE ATT&CK per ottenere informazioni sulle tattiche e sulle tecniche prevalentemente usate dai criminali e per rafforzare i playbook di conseguenza allo scopo di distruggere la kill chain del ransomware.

Aggiornare continuamente i sistemi di difesa e formate il personale affinché riescano a riconoscere e a rispondere in modo efficace alle potenziali minacce. Integrare solide misure di difesa del perimetro aziendale, la protezione degli endpoint, il filtraggio delle e-mail e una regolare gestione delle patch. Monitorare continuamente il traffico di rete, i registri di sistema e il comportamento degli utenti, oltre ad implementare pratiche di rilevamento delle minacce in grado di identificare gli attacchi ransomware.

Eseguire backup dei dati in modo regolare e sicuro, inclusi quelli isolati, per assicurarsi di poter ripristinare rapidamente le informazioni critiche nel caso di un attacco ransomware. Implementare l'MFA per tutti gli account utente in modo da aggiungere un ulteriore livello di sicurezza.

L'adozione di queste strategie di mitigazione complete consentirà di migliorare notevolmente la capacità delle istituzioni finanziarie di difendersi dalle varie minacce informatiche, garantire la continuità operativa, proteggere la reputazione delle aziende e conservare la fiducia dei clienti.

Conclusione

Mentre le istituzioni finanziarie adottano la trasformazione digitale per migliorare le customer experience, la loro efficienza operativa e il loro posizionamento rispetto alla concorrenza, si intensificano i problemi legati alla sicurezza, insieme alla crescente pressione di doversi muovere in uno scenario normativo in continua evoluzione. In questa edizione del rapporto SOTI, abbiamo esplorato le minacce persistenti ed emergenti che si trova ad affrontare il settore dei servizi finanziari, sottolineando la necessità di eseguire valutazioni continue e di migliorare le soluzioni per la sicurezza. Con le minacce che diventano sempre più sofisticate, è fondamentale stare al passo rafforzando i sistemi di difesa e perfezionando le strategie di sicurezza.

Mentre gli attacchi DDoS alle istituzioni finanziarie ora superano quelli sferrati contro il settore del gaming (per lungo tempo considerato il bersaglio principale), questa preoccupante tendenza sottolinea l'aumento dei rischi correlati. Altri fattori come l'hacktivismo e l'attuale situazione geopolitica hanno reso i servizi finanziari più vulnerabili che mai. Allo stesso tempo, la portata e la gravità del traffico generato dai siti di phishing e impersonificazione dei brand che prendono di mira le istituzioni finanziarie, insieme alla velocità con cui i criminali riescono a creare nuovi domini dopo aver messo fuori uso i siti legittimi, hanno raggiunto livelli estremamente alti. Tenere traccia di queste attività può richiedere alle organizzazioni numerose risorse e i team addetti alla sicurezza hanno bisogno di soluzioni che comprendono servizi di rimozione delle minacce, intelligence sulle minacce e funzionalità di rilevamento degli attacchi di phishing e impersonificazione dei brand su diversi canali digitali.

I consumatori e gli enti di controllo, spesso, ritengono responsabili le istituzioni finanziarie che hanno subito attacchi di phishing e altre truffe, anche se non sono direttamente in difetto, e, soprattutto, gli attacchi di phishing e impersonificazione dei brand sono, frequentemente, i primi segnali di ulteriori pericoli futuri, pertanto diventa fondamentale interrompere tempestivamente il ciclo degli attacchi. Compiere un'azione decisiva può fare la differenza per evitare di subire una violazione e per salvaguardare la reputazione e la fiducia dei clienti della vostra organizzazione.

Considerando che gli attacchi sferrati contro le istituzioni finanziarie sono inesorabili, salvaguardare le informazioni riservate per impedire il verificarsi di frodi e abusi rimane una sfida non da poco. L'adozione di un sistema di sicurezza come il modello Zero Trust è fondamentale per difendersi in modo efficace dagli attacchi di phishing che prendono di mira i dipendenti e per impedire che i ransomware si diffondano all'interno delle reti per raggiungere le risorse critiche, il tutto garantendo, al contempo, la conformità con le nuove normative e con quelle già esistenti.

Questo rapporto fornisce utili informazioni sulle ultime tendenze negli attacchi al settore dei servizi finanziari per consentire di rafforzare i sistemi di difesa. Restando all'erta e implementando le strategie descritte in questo rapporto, sarà possibile proteggere le organizzazioni e i clienti dalle crescenti minacce.

Per aggiornamenti sulla nostra ultima ricerca, è possibile consultare il nostro Security Research Hub.

Metodologia

DDoS (livello 7)

Questi dati descrivono gli avvisi a livello di applicazione relativi al traffico osservato tramite la nostra soluzione WAF (Web Application Firewall). Gli avvisi sugli attacchi DDoS al livello 7 vengono attivati quando si rilevano anomalie volumetriche all'interno di una serie di richieste a un sito web, un'applicazione o un'API protetta. Questi avvisi possono essere attivati sia da richieste dannose che non dannose. Di solito, le richieste in sé non sono dannose, tuttavia un elevato numero di richieste può nascondere uno scopo illecito. Gli avvisi non indicano la corretta riuscita di un attacco. Sebbene questi prodotti consentano un alto livello di personalizzazione, i dati qui presentati sono stati raccolti senza prendere in considerazione le configurazioni personalizzate delle proprietà protette.

I dati sono stati ricavati da uno strumento interno per l'analisi degli eventi di sicurezza rilevati sull'Akamai Connected Cloud, una rete di circa 340.000 server in più di 4.000 sedi su quasi 1.300 reti in oltre 130 paesi. I nostri team addetti alla sicurezza utilizzano questi dati, misurati in petabyte al mese, per effettuare ricerche sugli attacchi, segnalare comportamenti dannosi e includere ulteriori informazioni nelle soluzioni Akamai.

Questi dati hanno riguardato un periodo di 18 mesi, dal 1° gennaio 2023 al 30 giugno 2024.

DDoS (livelli 3 e 4)

La soluzione Akamai Prolexic Routed difende le organizzazioni dagli attacchi DDoS per bloccare le minacce e altro traffico indesiderato o dannoso prima che raggiungano le applicazioni, i data center e l'infrastruttura basata su Internet (pubblica o privata) ibrida e nel cloud, incluse tutte le porte e i protocolli utilizzati. Gli esperti del SOCC (Security Operations Command Center) di Akamai personalizzano i controlli di mitigazione proattivi per rilevare e bloccare immediatamente gli attacchi ed eseguono analisi del traffico rimanente in tempo reale per determinare ulteriori misure di mitigazione, in base alle necessità. Questi attacchi mitigati sono organizzati e raggruppati in eventi di attacco, i cui dati associati vengono registrati dal SOCC per l'analisi.

I dati inclusi in questo rapporto hanno riguardato un periodo di 18 mesi, dal 1° gennaio 2023 al 30 giugno 2024, salvo altrimenti specificato.

Attacchi di impersonificazione dei brand

Akamai Brand Protector, una soluzione che consente di difendersi dagli abusi, è stata progettata per proteggere le aziende e i loro clienti dagli attacchi di impersonificazione dei brand, inclusi siti web contraffatti, tentativi di phishing, falsi account sui social media e applicazioni non autorizzate. Utilizzando la rete edge globale di Akamai, la soluzione analizza più di 900 TB di dati ogni giorno per rilevare le minacce prima che influiscano sui clienti. Queste informazioni vengono arricchite con dati provenienti da partner di terze parti in modo da offrire una visione più ampia delle potenziali minacce sulle varie piattaforme online.

Vengono analizzate diverse caratteristiche di ciascuno dei domini sospetti rilevati e i livelli di rischio determinati contribuiscono a raggiungere il punteggio di pericolosità calcolato per i domini. Questi domini sospetti vengono monitorati, insieme ai dati associati, mentre i clienti interessati vengono avvisati relativamente a queste campagne dannose che tentano di sfruttare le identità dei brand.

I dati inclusi in questo rapporto hanno riguardato i domini sospetti rilevati in un periodo di 12 mesi, dal 1° agosto 2023 al 31 luglio 2024.

Riconoscimenti

Direttore della ricerca

Mitch Mayne

Editoria e stesura

James Casey
Lance Rhodes
Badette Tribbey

Revisione e contributi di esperti del settore

Cheryl Chiodi
Ziv Eli
Reuben Koh
Gal Meiri
Richard Meeus
Steve Winterfeld

Analisi dei dati

Chelsea Tuttle

Materiali promozionali

Barney Beal

Marketing ed editoria

Georgina Morales
Emily Spinks

Altri rapporti sullo stato di Internet - Security

È possibile leggere i numeri precedenti e consultare le prossime pubblicazioni degli acclamati rapporti sullo stato di Internet - Security di Akamai sul sito **akamai.com/soti**

Ulteriori informazioni sulla ricerca delle minacce di Akamai

Sono disponibili ulteriori aggiornamenti sulle ultime novità in materia di intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza consultando il sito **akamai.com/security-research**

Accesso ai dati del rapporto

È possibile visualizzare i grafici e i diagrammi citati in questo rapporto in versioni di alta qualità. L'utilizzo e la consultazione di queste immagini sono forniti a scopo gratuito, purché Akamai venga debitamente citata come fonte e venga conservato il logo dell'azienda: **akamai.com/sotidata**

Ulteriori informazioni sulle soluzioni di Akamai

Per ulteriori informazioni sulle soluzioni Akamai contro le minacce che prendono di mira il settore dei servizi finanziari, è possibile visitare la nostra **pagina dedicata ai servizi finanziari**.