
corero
[NETWORK SECURITY]
2025
RAPPORTO SULL'INTELLIGENZA DELLE MINACCE

Prefazione del CTO

Ashley Stephenson
Direttore della tecnologia e dei prodotti Corero Network Security

Ogni anno i dati raccontano una storia. Non solo su cosa fanno gli aggressori, ma anche su cosa sono disposti a scommettere. Nel 2024, puntano su velocità, automazione e accesso. E perché non dovrebbero? Gli strumenti sono poco costosi. L'infrastruttura è ovunque. Le barriere sono basse. Ciò che prima richiedeva un coordinamento sofisticato ora può essere realizzato sempre più spesso con pochi dollari, una botnet a noleggio e un codice malware riciclato o replicato dall'intelligenza artificiale.

Noi di Corero seguiamo le tendenze DDoS da anni. E se alcune tendenze ci sono familiari - gli attacchi rapidi e brevi dominano ancora - ci sono sfumature che richiedono attenzione. La frequenza è in aumento. Il volume sta salendo ancora. La parte centrale dello spettro degli attacchi si sta assottigliando. Ciò che rimane è una miscela di pressione opportunistica e forza bruta strategica, alimentata dall'automazione e dall'adattamento costante.

E così come si evolvono gli aggressori, si evolve anche l'architettura che prendono di mira. Con l'aumento degli ambienti cloud ibridi e la tendenza a rimpatriare i carichi di lavoro critici nell'infrastruttura on-prem, la complessità della difesa sta crescendo. I percorsi del traffico sono meno prevedibili. I punti di applicazione sono più distribuiti. E per molte organizzazioni questo significa più punti ciechi o porte lasciate "aperte".

Il rapporto di quest'anno riflette non solo ciò che vediamo nei dati, ma anche ciò a cui ci stiamo preparando. Gli attori delle minacce non sono più limitati dalla larghezza di banda o dalla geografia. Stanno costruendo infrastrutture più intelligenti, riutilizzando continuamente dispositivi compromessi e prendendo sempre più di mira il livello delle applicazioni. In qualità di difensori, dobbiamo abbinare questa adattabilità a visibilità, automazione e velocità.

Questa complessità si traduce in nuove sfide per la risposta dei difensori. Secondo uno studio di Merrill Research, molti team riferiscono di avere difficoltà a coordinarsi tra gli ambienti, a tenere il passo con le minacce e ad eseguire rapidamente le operazioni. La sfida non è solo il volume degli attacchi, ma anche l'attrito operativo che rallenta la difesa.

La nostra missione in Corero è dare alle organizzazioni il potere di vedere, fermare ed anticipare più velocemente minacce che devono affrontare. Questa missione non è mai stata così urgente.

Grazie per aver letto e per far parte della comunità che difende ciò che conta.

Sintesi

Nel 2024, gli aggressori DDoS non hanno reinventato il loro manuale, ma lo hanno perfezionato. I dati raccontano una storia di attacchi incessanti e ad alta frequenza portati avanti con un'efficienza e una scala sorprendenti. Gli attacchi rapidi e brevi, al di sotto dei 10 Gbps, hanno continuato a dominare, come hanno fatto per anni, sottolineando un modello di minaccia persistente e in evoluzione in cui l'interruzione è economica, accessibile e allarmantemente efficace.

La nostra analisi dei modelli di traffico dei clienti mostra che le organizzazioni da noi monitorate hanno affrontato una media di 11 attacchi DDoS al giorno nel 2024, con un aumento del 5% rispetto all'anno precedente. La maggior parte di questi attacchi era di dimensioni inferiori a 1 Gbps, in grado di scivolare sotto le soglie volumetriche tradizionali anche se riescono a interrompere la disponibilità e le prestazioni. Questi risultati rafforzano una tendenza che abbiamo osservato anno dopo anno: la frequenza è l'arma preferita dagli aggressori.

Se da un lato dominano gli attacchi di piccole dimensioni, dall'altro si registra un'impennata degli attacchi su larga scala. Gli attacchi che superano i 10 Gbps sono saliti al 2,9% di tutti gli eventi osservati, il valore più alto dal 2018. Riteniamo che ciò rifletta un aumento della capacità e dell'automazione delle botnet, guidato dallo sfruttamento di dispositivi vulnerabili come i router MikroTik e i derivati malware Mirai in esecuzione su dispositivi di tipo IoT.

Allo stesso tempo, gli attacchi di medie dimensioni, tra i 5Gbps e i 10Gbps, continuano a diminuire, dal 19% nel 2019 ad appena il 12,4% nel 2024. Il "livello intermedio" degli attacchi DDoS sta scomparendo a causa della polarizzazione degli aggressori: molti di essi utilizzano il probing onnipresente a basso volume per testare le difese, mentre altri scatenano campagne strategiche ad alto volume per sopraffare infrastrutture specificamente mirate.

L'analisi trimestrale rivela una costante stagionalità. Il terzo e il quarto trimestre rimangono i periodi di picco per l'attività di attacco, in linea con le stagioni ad alto traffico commerciale e le finestre potenzialmente sovraccariche di personale. È interessante notare che il secondo trimestre del 2024 ha visto un numero inferiore di attacchi in generale, ma una percentuale più elevata di attacchi di grandi dimensioni, un possibile segnale di ricognizione o di test in fase di preparazione di campagne più ampie.

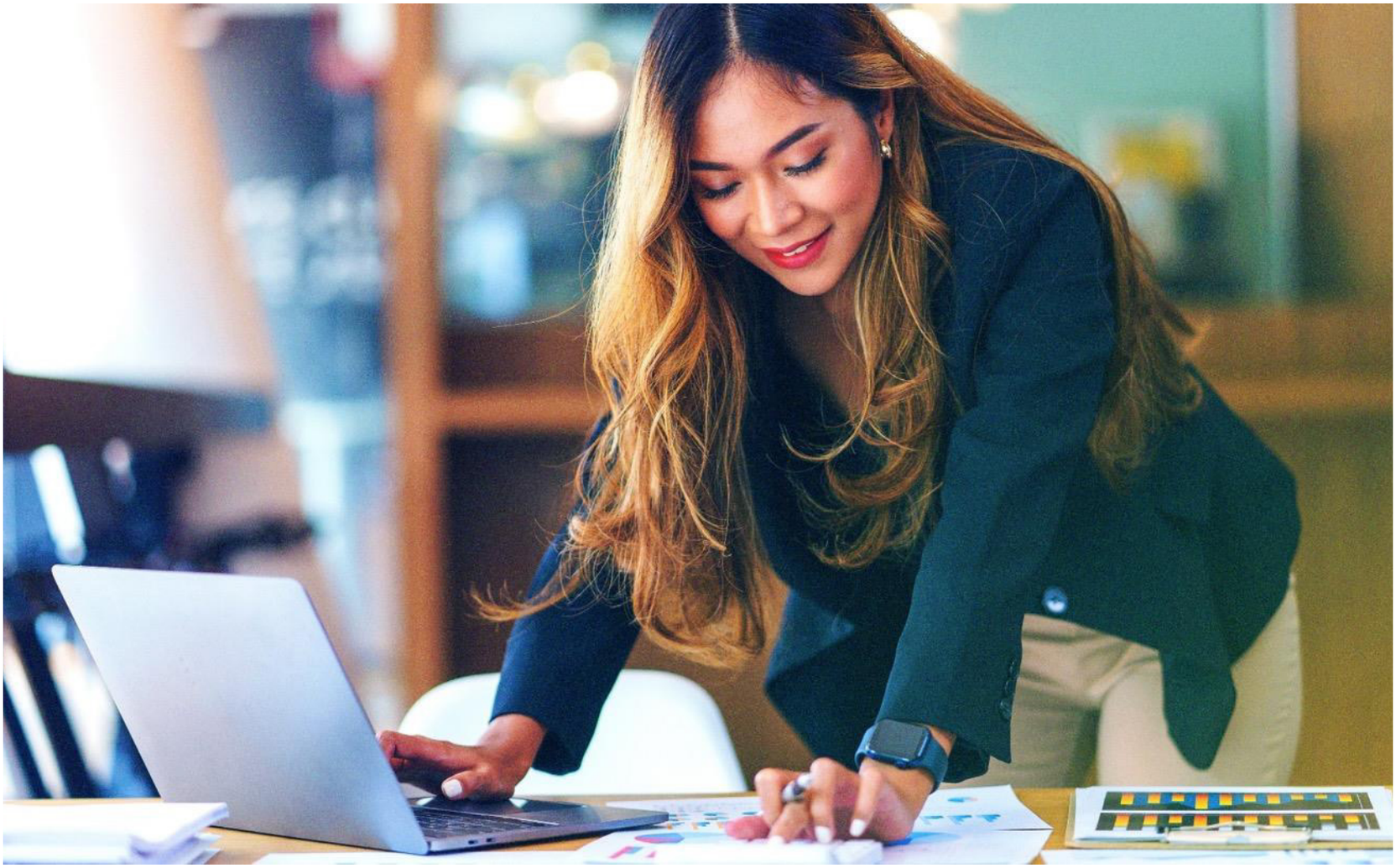
Anche gli attacchi di livello applicativo (Layer 7) sono in aumento in tutto il settore. Le inondazioni HTTP, il targeting delle API e le campagne DDoS specifiche per piattaforma stanno diventando sempre più comuni, poiché gli aggressori cercano di distruggere oltre la semplice saturazione della larghezza di banda. Poiché le difese delle applicazioni diventano la prossima linea del fronte, le organizzazioni devono essere preparate a difendere non solo la rete, ma la stessa logica aziendale.

Il risultato è chiaro:

Il DDoS sta diventando uno stato di costante pressione di fondo. Gli aggressori si affidano all'automazione, alla convenienza economica e alla distribuzione su scala infrastrutturale per mantenere le vittime in una posizione reattiva di "whack-a-mole". Ciò che ha sempre funzionato funziona ancora. Finché i difensori non si metteranno al passo in termini di velocità, visibilità e automazione, il DDoS rimarrà uno degli strumenti più efficaci e persistenti nell'arsenale degli aggressori.

Attaccare con DDoS è facile. Difendersi, ancora no.

Leggere Tra i Pacchetti



Ogni attacco lascia una traccia. Nel 2024, la nostra telemetria globale ha catturato centinaia di migliaia di queste tracce - modelli in termini di frequenza, volume, tempistica e tattiche - provenienti da attacchi reali che hanno preso di mira reti di produzione reali.

Questa sezione non è solo un resoconto di ciò che è accaduto. Abbiamo esaminato non solo il 2024, ma più anni di dati storici per far emergere modelli, cambiamenti e strategie persistenti che danno forma al panorama delle minacce. È un'interpretazione di ciò che questi modelli significano per i difensori. Perché dietro ogni punto di dati c'è una decisione: di un attaccante, di un difensore o di un sistema costretto a scegliere cosa bloccare e cosa consentire.

Nelle pagine che seguono, analizziamo le tendenze che secondo noi definiscono il 2024: cosa dicono i dati, perché sono importanti e cosa possono fare i difensori in risposta. È qui che i numeri incontrano il mondo reale e che inizia la vera strategia.

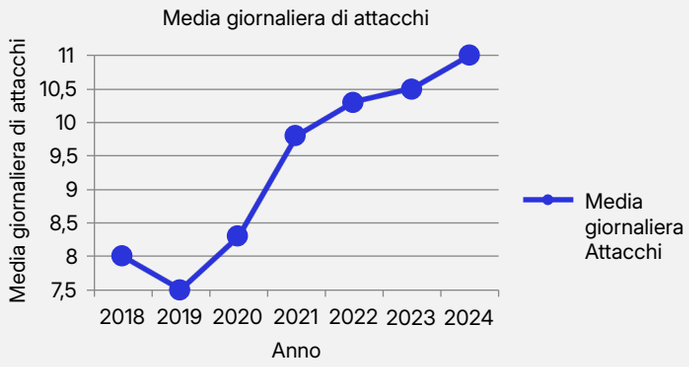
Vediamo di cosa dispongono gli aggressori.

Il Ritmo della Pressione:
Frequenza Giornaliera degli Attacchi DDoS

COSA DICONO I DATI

Nel 2024, i clienti Corero hanno registrato un media di 11 attacchi DDoS al giorno, in aumento rispetto a 10,48 nel 2023. Si tratta di un aumento del 5% su base annua e di tendenza pluriennale più ampia. Dal 2018, la media giornaliera è salita costantemente da circa 8 a 11 attacchi giorno per cliente, con un aumento del 37,5% in sei anni.

Attacchi DDoS medi giornalieri per cliente (2018-2024)



COSA SIGNIFICA

Non si tratta di un picco, ma di una strategia. La frequenza degli attacchi non è casuale, ma deliberata. Con l'aumento del numero di aggressori, aumenta anche la pressione di fondo continua, che utilizza l'automazione e l'armamento dell'infrastruttura a basso costo per mantenere le difese attive, sopraffattee o desensibilizzate.

Molti di questi attacchi ad alta frequenza sono di breve durata e poco saturi, il che li rende facili da liquidare come rumore di fondo. Ma servono a scopi fondamentali:

- Sondare i punti deboli
- Misurazione delle soglie di mitigazione
- Ritardi nella risposta ai tempi
- Distrarre i team di sicurezza da altre attività attività mirate

In parole povere:

Se state difendendo 11 attacchi al giorno, non state rispondendo a un'anomalia...si opera in un ambiente di fuoco vivo.

Il Ritmo della Pressione

COSA POTETE FARE

Le organizzazioni devono trattare gli attacchi frequenti come una condizione predefinita, non un'eccezione. Azioni chiave includono:

- Automatizzare i flussi di risposta per rilevare e mitigare senza intervento umano.
- Migliorare la sensibilità di rilevamento per identificare anomalie di breve durata e sotto soglia.
- Stabilire una migliore comprensione del comportamento normale del traffico, in modo da identificare le deviazioni con maggiore precisione.
- Rafforzare l'infrastruttura ai margini per assorbire o deviare attacchi ad alta frequenza e basso volume senza consumare risorse interne preziose.

È un'anomalia o un attacco DDoS?

Come si fa a sapere che si è sotto attacco quando Gli indicatori sembrano rumore?

È proprio questo il problema. La maggior parte degli attacchi che osserviamo, soprattutto quelli inferiori a 1 Gbps, non causano necessariamente interruzioni evidenti. Creano invece latenza, perdita di pacchetti o interruzioni transitorie che assomigliano a una serie di problemi di rete comuni. Molte organizzazioni li considerano come inconvenienti dell'ISP o normali condizioni atmosferiche di Internet.

Ma ecco cosa distingue questi eventi come attacchi:

1. Seguono degli schemi: forse l'ora del giorno, caratteristiche di protocollo simili, stessa fonte o stesse regioni.
2. Coincidono con campagne di scansione, sondaggio o riempimento di credenziali più ampie.
3. Scompaiono o si spostano rapidamente quando le difese si attivano - un comportamento anomalo per interruzioni reali.
4. Tornano più volte, spesso con un firma diversa.

Se si osserva uno schema di interruzioni di breve durata e apparentemente minori, è possibile che non si tratti di un'infrastruttura inaffidabile.

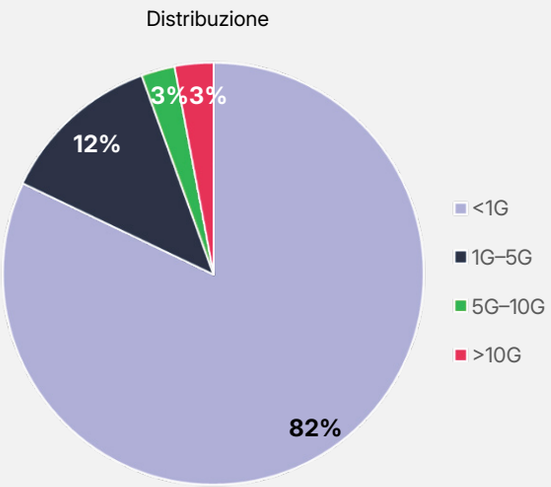
Potreste avere a che fare con un aggressore che sta testando i vostra limiti.

Sotto il Radar, Oltre il Limite:
La Persistenza degli Sttacchi Sub-10Gbps

COSA DICONO I DATI

Oltre l'82% di tutti gli attacchi DDoS osservati nel 2024 erano di dimensioni inferiori a 1 Gbps. Questi attacchi su piccola scala sono di gran lunga il tipo più comune di attacchi in natura. Spesso considerati come rumore di fondo, persistono perché sono più facili da lanciare, più difficili da rilevare e più efficaci nel degradare la qualità complessiva del servizio o nel testare i limiti di una difesa.

Distribuzione delle dimensioni degli attacchi DDoS - 2024



COSA SIGNIFICA

Piccoli attacchi non significano un impatto ridotto. Queste campagne da meno di 10 Gbps possono ancora mettere in crisi servizi applicativi fragili, esaurire i firewall o innescare operazioni di scaling inutili e costose in ambienti cloud. Sono efficienti e, in molti , precursori minacciosi di campagne più grandi. È inoltre importante notare che questi numeri non rappresentano necessariamente attacchi discreti e sicuramente ci sono casi in cui un aggressore può aver lanciato diversi piccoli attacchi che si aggregano in un attacco totale più grande.

I difensori spesso non riescono a individuare questi attacchi non perché siano intrinsecamente furtivi, ma perché operano in una zona grigia difficilmente monitorata. Non è detto che facciano scattare allarmi volumetrici di ampia portata o che causino interruzioni immediatamente identificabili. Invece, si muovono con leggerezza, producendo impronte deboli: ritardi nel caricamento delle pagine, errori 5xx intermittenti, singhiozzi o guasti DNS momentanei. Questi effetti possono essere facilmente ignorati come rumori casuali di Internet, ma se considerati nel contesto, spesso indicano un sondaggio coordinato o una degradazione deliberata.

L'implicazione per i difensori è chiara: non si tratta di artefatti di fondo, ma di segnali validi di attacchi potenzialmente più dirompenti. Il modo migliore per farli emergere è il monitoraggio comportamentale e la correlazione nel tempo e tra i sistemi. È qui che la visibilità operativa, non solo la difesa basata sulla larghezza di banda, diventa fondamentale.

Sotto il Radar, Oltre il Limite

COSA POTETE FARE

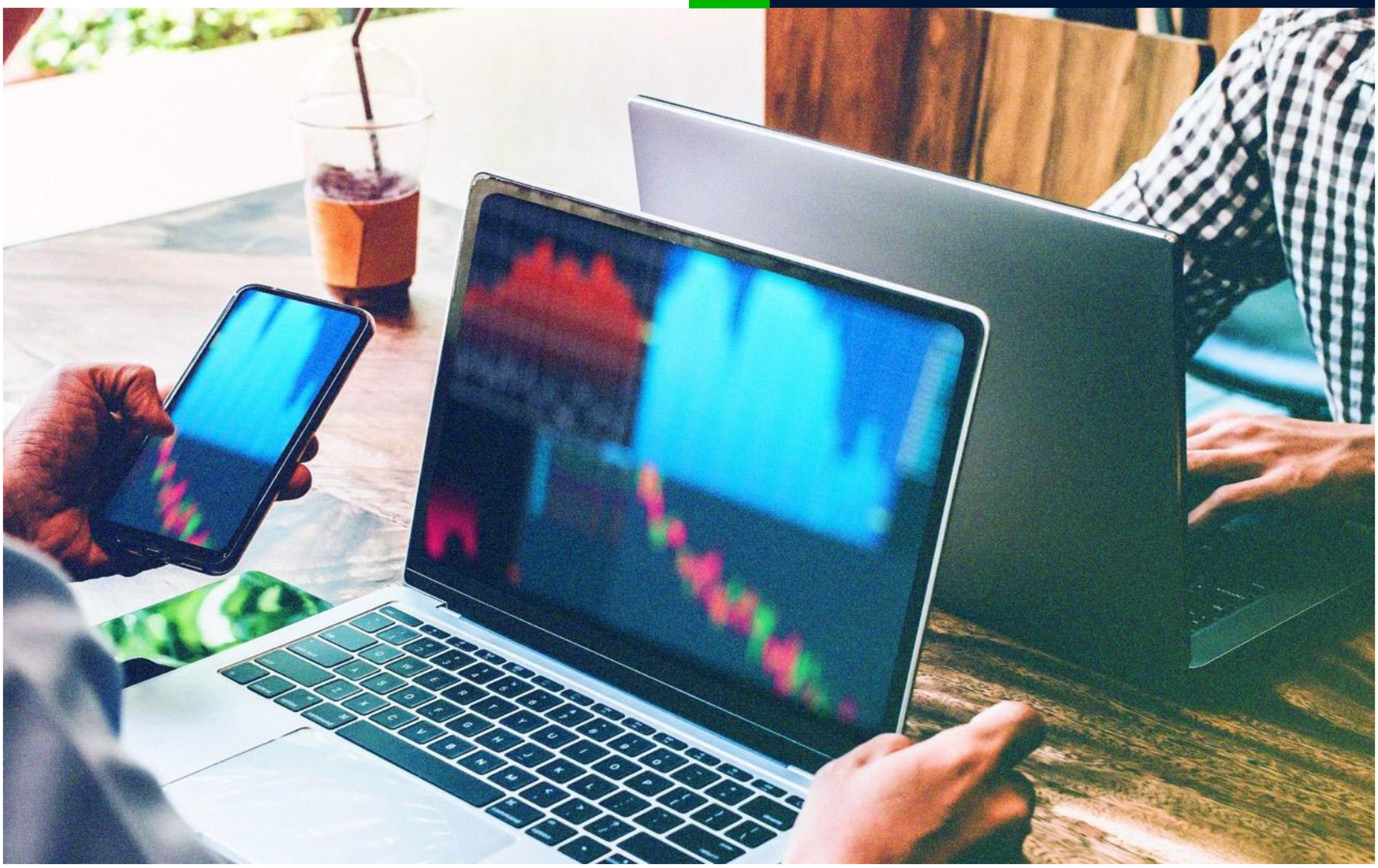
Cercate le anomalie delle prestazioni, come i picchi di latenza o le interruzioni inspiegabili del servizio, come indicatori precoci.

Correlare gli eventi in tutto l'ambiente per campagne a basso volume e su più fronti.

Regolare le soglie di allarme per catturare meglio le interruzioni piccole e persistenti che eludono i trigger volumetrici.

Test o obiettivo?

I piccoli attacchi non sono necessariamente grandi attacchi falliti. Molti sono sonde. Alcuni sono progettati per testare le soglie di rilevamento. Altri mirano ad applicazioni specifiche con una pressione sufficiente a causare instabilità. Per capire la differenza tra test e obiettivo è necessario un contesto. E il contesto deriva dalla visibilità, dalla telemetria e dalle indagini.



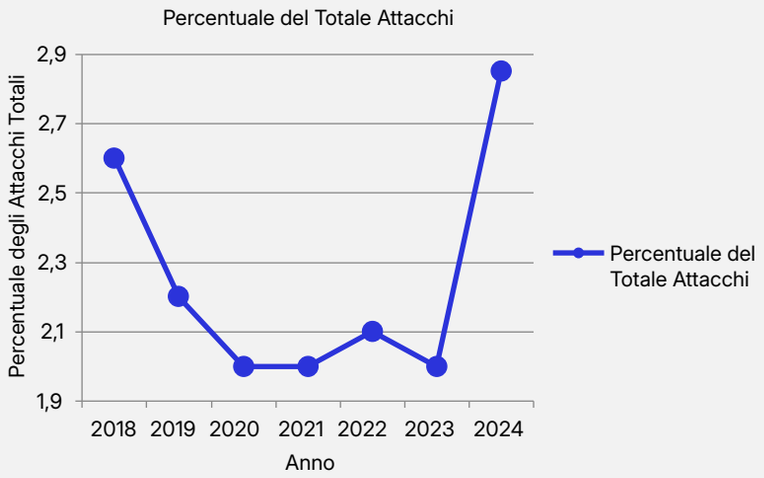
Il Ritorno di Botnet Più Potenti:
Aumento degli Attacchi >10Gbps

COSA DICONO I DATI

Nel 2024, il 2,9% di tutti gli attacchi DDoS osservati hanno superato i 10 Gbps di dimensione. Si tratta della quota più alta di attacchi su larga scala dal 2018, dopo diversi anni di andamento relativamente piatto di queste attività.

Anche se questi eventi rimangono rari rispetto a La categoria dominante dei sub-1Gbps, il loro potenziale di interruzione è notevole e spesso si rivolge a punti di strozzatura dell'infrastruttura, limiti di capacità a valle o accordi sui livelli di servizio.

Crescita degli Attacchi DDoS >10Gbps (2018-2024)



COSA SIGNIFICA

Questa crescita indica che la potenza di fuoco delle botnet sta aumentando di nuovo e che gli aggressori stanno ottenendo accesso a un numero maggiore di dispositivi o di orchestrare meglio quelli che già controllano.

I fattori che contribuiscono sono probabilmente:

- Sfruttamento di router e IoT vulnerabili dispositivi, come l'hardware MikroTik
- Continua evoluzione e rinascita di Malware basato su Mirai
- Crescente utilizzo di servizi DDoS a noleggio con capacità di attacco multivettoriale

Questi attacchi più grandi sono spesso:

- Usati come paravento per i dati esfiltrazione o movimento laterale
- Tempistica per massimizzare l'interruzione operativa (ad es, ore di punta o durante gli incidenti)
- In combinazione con le richieste di riscatto, le minacce di attacchi ripetuti o prolungati

Il Ritorno di Botnet Più Potenti

COSA POTETE FARE

- Conoscere i limiti di capacità. Ciò che il vostro ISP può assorbire ≠ ciò che la vostra infrastruttura può tollerare.
- Collaborare con i fornitori a monte per comprendere le opzioni di reindirizzamento, scrubbing e failover degli attacchi.
- Testate la vostra risposta di mitigazione a eventi simulati su larga scala (non solo volumetrici, ma multivettoriali).
- Non date per scontato che la rarità sia sinonimo di sicurezza. Gli attacchi possono essere meno numerosi, ma il loro impatto sui ricavi, sulle operazioni e sulla reputazione può essere grave.

Perché le Dimensioni Maggiori Non Sono Sempre Più Distruttive

Gli attacchi su larga scala fanno notizia, ma non sempre sono progettati per distruggere Internet. Alcuni sono usati come cortine fumogene, per mascherare intrusioni più sottili. Altri sono temporizzati in modo da causare la massima operatività stress, al cambio di turno, durante le ore di punta, o in in concomitanza con le richieste di ransomware.

A rendere pericolosi questi attacchi non è solo la loro larghezza di banda. È il loro modello di bersaglio, la tempistica e l'interruzione che creano al di là della rete, dalla stanchezza per gli allarmi al panico dei dirigenti.

Non confondete la rarità con l'irrilevanza. I grandi attacchi sono armi strategiche e sono tornati nell'arsenale.

Quando Arrivano le Tempeste:
Stagionalità dei DDoS e Tempistica Strategica

COSA DICONO I DATI

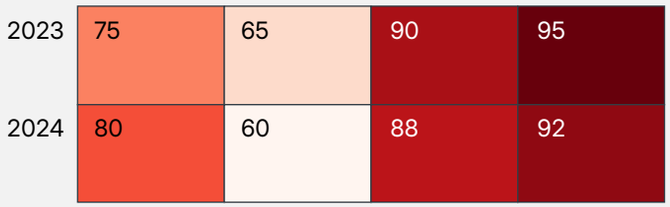
Tra il 2023 e il 2024, Corero ha osservato picchi ricorrenti nel volume degli attacchi durante il terzo e il quarto trimestre.

In entrambi gli anni:

- Nel terzo trimestre si è registrato un aumento della frequenza totale degli attacchi, in particolare i burst a meno di 1 Gbps.
- Il quarto trimestre ha mostrato un mix più ampio di dimensioni degli attacchi, inclusa una maggiore concentrazione di eventi superiori a 1 Gbps.

Al contrario, nel secondo trimestre del 2024 si è registrata una diminuzione della frequenza, ma una quota maggiore di attacchi su larga scala, compresi eventi superiori a 10 Gbps.

Attività di attacco DDoS per trimestre



COSA SIGNIFICA

Gli aggressori non operano nel vuoto: rispondono ai ritmi aziendali, agli eventi del calendario e alle pressioni operative.

I principali modelli stagionali possono includere:

Q3 Incremento del back-to-school e del periodo pre-vacanziero (mirato a giochi, vendita al dettaglio, istruzione)

Q4 Il perdel personale e un riodo delle vac ianztardo nelle rispose e il blocco delle modifiche ITte. , che spesso coincidono con una riduzione

Queste tendenze suggeriscono che la tempistica degli attacchi sta diventando più strategica, allineandosi ai momenti in cui le interruzioni fanno più male.

Quando Arrivano le Tempeste

COSA POTETE FARE

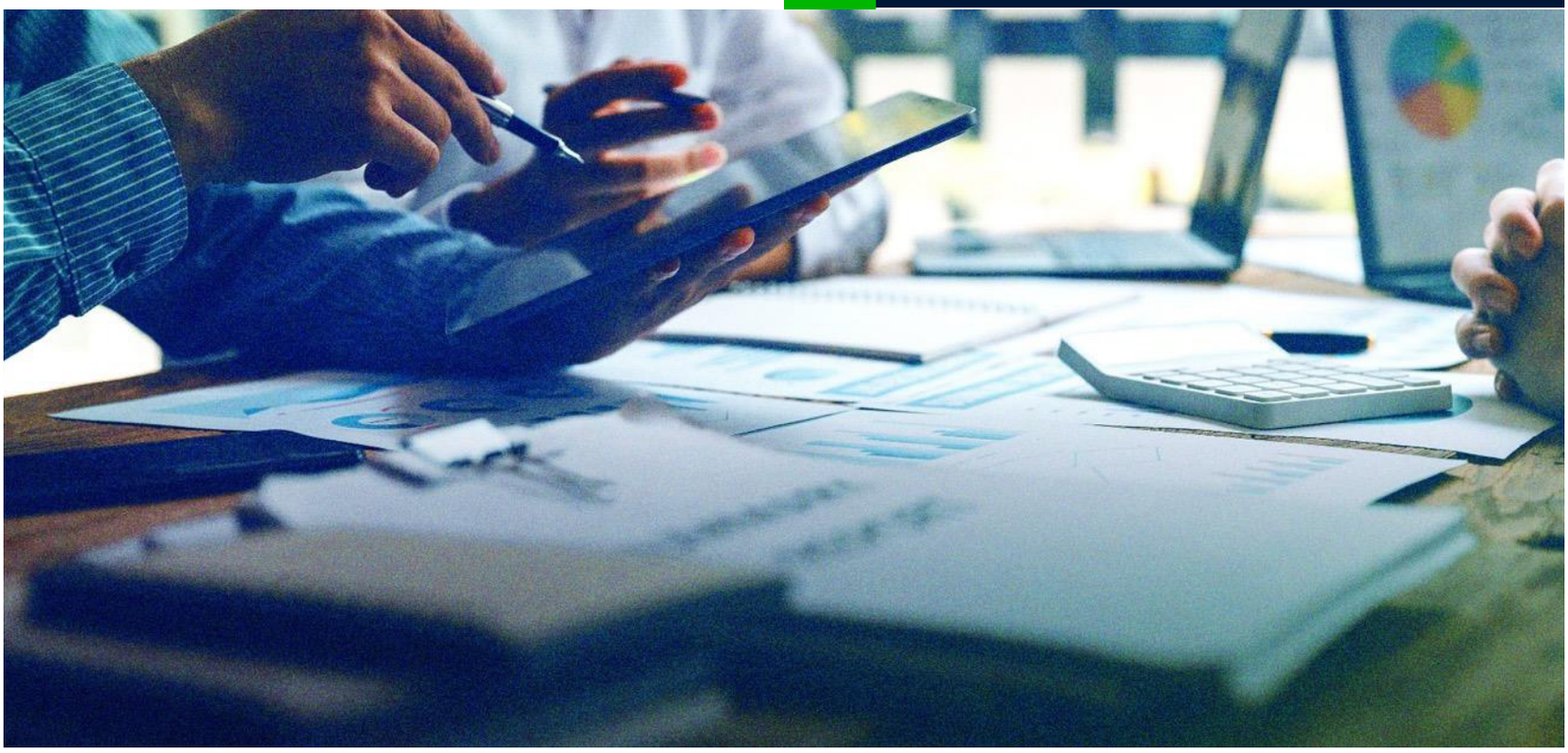
- Staffa le tue difese tenendo conto della stagionalità. Pianifica un aumento delle attività a fine Q3 e Q4.
- Sfrutta i periodi di bassa attività come Q1 e Q2 per rafforzare la tua infrastruttura e testare i flussi di lavoro di mitigazione.
- Allinea gli esercizi di red team/blue team con i picchi noti di DDoS per garantire copertura e fiducia.
- Non fare affidamento solo sulle tendenze medie—osserva la stagionalità storica per prevedere i momenti di maggiore pressione.

Quando I Difensori Chiudono Gli Occhi

Il quarto trimestre è una delle stagioni preferite dagli aggressori, non tanto perché fa freddo, ma perché i team di sicurezza sono in affanno. I budget sono congelati. Il personale è fuori per le ferie. E le finestre di cambiamento sono limitate dalla tolleranza al rischio aziendale.

Gli aggressori lo sanno. Sfruttano la tempistica quanto gli strumenti, lanciando campagne DDoS quando i tempi di risposta sono più lenti e la tolleranza alle interruzioni più bassa.

Se le vostre difese dipendono dal fatto che le persone sono presenti, riposate e pronte, allora la stagionalità non è solo uno schema, ma un'opportunità per l'avversario.



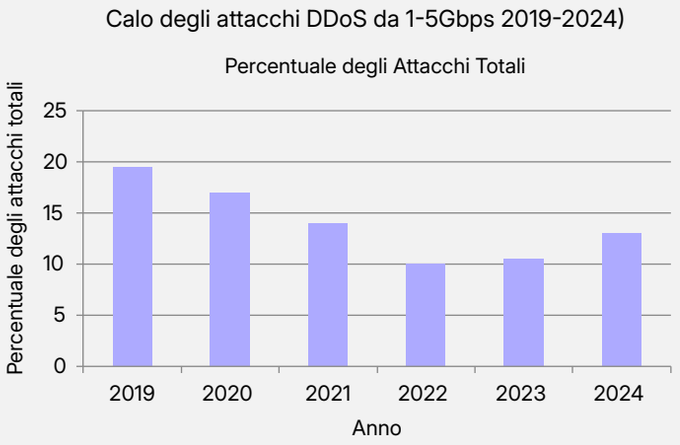
Il Centro Misterioso:
Il Declino Degli Attacchi a 1-5Gbps

COSA DICONO I DATI

Nel 2019, gli attacchi nella fascia 1-5Gbps hanno rappresentato quasi il 19,4% di tutti gli eventi DDoS osservati. Entro il 2024, questo numero è sceso ad appena il 12,4%, con una riduzione del 34% della quota in cinque anni.

Anche se ci sono stati alcuni cambiamenti da un anno all'altro la tendenza a lungo termine per questo livello è in calo, passando dal 19,4% nel 2019 al 12,8% nel 2024.

Forse è solo superata dalla crescita degli attacchi di fiancheggiamento.



COSA SIGNIFICA

Questa tendenza segnala una polarizzazione strategica nell'attaccante ma il motivo rimane ancora speculativo. Ecco la nostra opinione:

Molti aggressori optano per attacchi a basso volume e alta frequenza che evitano il rilevamento e la risposta ai test.

Altri potrebbero investire in inondazioni su larga scala e ad alto impatto, grazie a botnet e infrastrutture pay-to- play.

Il livello intermedio sta diventando obsoleto perché inefficace o non più efficiente?

La gamma 1-5Gbps:

- E' troppo piccolo per schiantarsi contro le infrastrutture moderne.
- Ma troppo grande per passare inosservato
- Meno efficiente rispetto ad altre opzioni

L'allontanamento dalla fascia centrale potrebbe riflettere l'evoluzione dei difensori. A nostro avviso, la fascia da 1 a 5 Gbps era un punto cieco per molti provider: abbastanza grande da danneggiare, ma abbastanza piccolo da passare inosservato. Ma con la maturazione della protezione DDoS, questa finestra si è ristretta.

Gli aggressori se ne sono accorti. Oggi non sprecano larghezza di banda dove è probabile che venga segnalata e filtrata. Si fanno grandi per sopraffare o piccoli per passare inosservati.

Per i difensori, la rete consiste nel ricalibrare le aspettative. Se la vostra postura di rilevamento e risposta è ancora orientata a catturare le inondazioni di medio livello, potreste essere sovraccarichi di risorse per ciò che non è più comune e poco preparati per i casi limite.

Il Centro Misterioso

COSA POTETE FARE

Osservate i bordi, non solo il centro. La logica di rilevamento deve concentrarsi sui modelli di burst e sulle anomalie, non solo sulle soglie fisse.

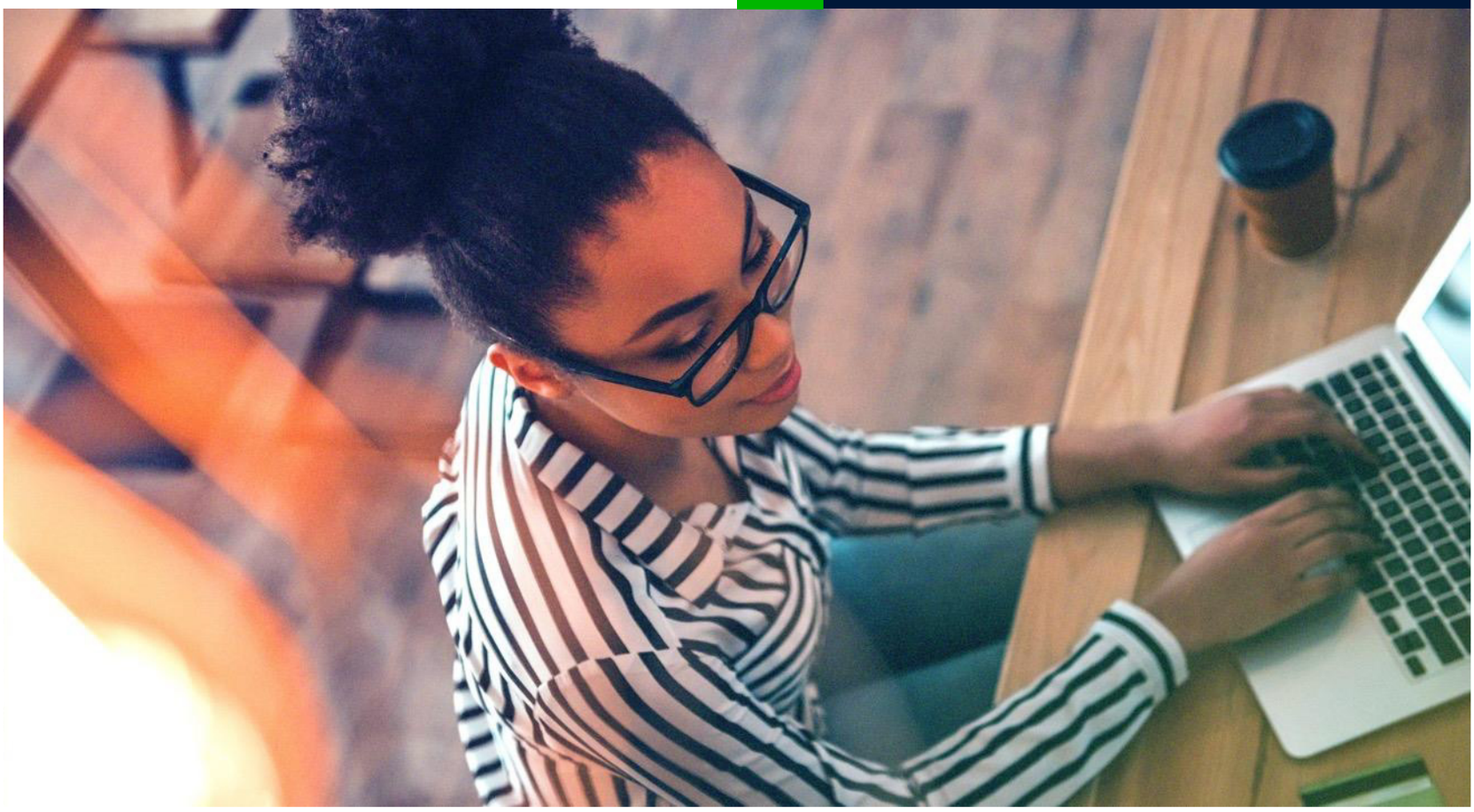
Valutate la vostra posizione difensiva ai due estremi dello spettro: siete in grado di gestire migliaia di piccoli burst? Siete in grado di assorbire un colpo da 20 Gbps?

Verificate la messa a punto della mitigazione per evitare di spendere risorse eccessive su attacchi che non sono più prevalenti, ma non eliminate del tutto la copertura.

Il Centro DDoS è Sparito

Il "livello intermedio" DDoS si sta riducendo come percentuale di tutti gli attacchi. Un tempo questi attacchi rappresentavano un equilibrio strategico: abbastanza grandi da avere un impatto sulle prestazioni, ma abbastanza piccoli da evitare un rilevamento immediato.

Riteniamo che gli aggressori stiano ottimizzando il ROI. Gli attacchi sub-1Gbps sono più economici e chirurgici, mentre le inondazioni >10Gbps sono più drammatiche e dirompenti. La fascia 1-5Gbps? È sempre più abbandonata.



Gli Attacchi si Stanno Evolvendo:
Campagne DDoS Più Intelligenti e Adattive

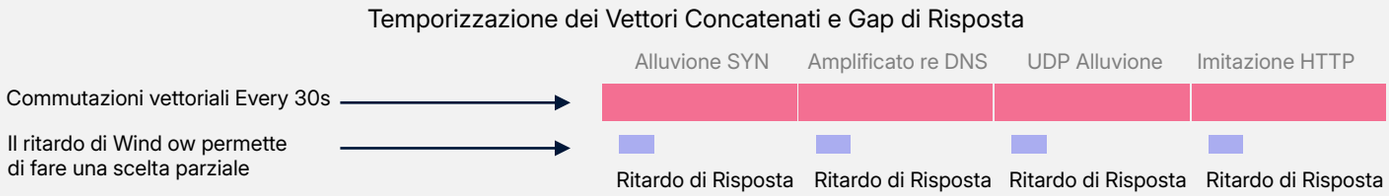
COSA DICONO I DATI

Abbiamo osservato un modello crescente di campagne DDoS multivettore, sequenziali ed evasive per tutto il 2024. Mentre il volume da solo non è più il fattore determinante, il comportamento degli aggressori sta diventando più sofisticato. In molti casi, gli aggressori hanno lanciato attacchi coordinati che hanno colpito diverse sottoreti contemporaneamente o in rapida successione, spesso combinando più vettori in brevi raffiche. Queste campagne non solo sono più difficili da rilevare, ma mirano anche a sfruttare le lacune dei sistemi di rilevamento e mitigazione.

Questo comportamento comprende:

- Rapido cambio di vettore (ad esempio, alternando SYN flood, amplificazione DNS e HTTP mimic).
- Testare le difese sondando i punti deboli e modificando le tattiche.
- Lancio di attacchi ad alto volume con microburst per aggirare le soglie statiche

In diverse campagne osservate, gli aggressori hanno impiegato quelli che qui descriviamo come "vettori concatenati": attacchi in stretta sequenza che passano rapidamente da un protocollo all'altro ogni 30-60 secondi. Anche se ogni vettore, preso singolarmente, può essere gestibile, la tempistica e il coordinamento sono progettati per sfruttare anche brevi ritardi nel rilevamento o nella mitigazione, mantenendo le difese proattive piuttosto che reattive.



COSA SIGNIFICA

Questa evoluzione indica che gli aggressori non puntano più solo all'interruzione, ma cercano di superare l'automazione. Il passaggio dalla forza bruta all'adattabilità strategica mette a dura prova anche le strutture di mitigazione più reattive.

Le difese tradizionali sono spesso costruite per rilevare il volume, non la velocità. Ogni volta che un attaccante cambia tattica, ad esempio passando dall'apertura di false connessioni TCP all'attivazione dell'amplificazione DNS o al lancio di flood UDP, la difesa deve fermarsi, rivalutare e riclassificare. Questo ciclo, per quanto breve, crea ripetuti punti ciechi.

Abbiamo osservato campagne che ruotano i vettori proprio quando si attiva l'attenuazione, creando un effetto di rotazione che lascia i team SOC a rincorrere la coda dell'attacco. Non si tratta di rumore. È un progetto. La capacità di rilevare l'intento, non solo i pacchetti, sta diventando essenziale.

Gli Attacchi si Stanno Evolvendo

COSA POTETE FARE

Individua schemi a breve termine: Usa la tua telemetria per identificare rapidi cambiamenti nel tipo di protocollo, nel targeting delle porte o nella dimensione dei pacchetti. Questi cambiamenti—soprattutto se si verificano ogni 30–60 secondi—possono indicare un comportamento a catena di vettori.

Tagga e segnala le anomalie in tempo reale: Sviluppa regole o script leggeri che tagghino i nuovi profili di traffico non appena emergono. Questo aiuta a creare cicli di feedback rapidi per il tuo SOC, anche prima che i cicli di rilevamento completi siano terminati.

Costruisci manuali SOC basati sul comportamento degli attaccanti: Usa i modelli a catena noti per informare i tuoi flussi di lavoro di escalation. Stabilisci aspettative interne su cosa significhi un ritmo di risposta 'normale' e cosa potrebbe segnalare qualcosa di più coordinato.

Perché il cambio di vettori funziona

Negli ambienti di mitigazione odierni, il tempo è tutto. La maggior parte delle difese DDoS si basa su firme di rilevamento, soglie di velocità e riconoscimento di modelli che richiedono tempo per attivarsi. Anche le piattaforme più avanzate possono impiegare 10-30 secondi, o più, per analizzare il traffico e iniziare la mitigazione.

Gli attaccanti sfruttano questo aspetto. Cambiando vettore ogni 30-60 secondi, loro:

- Eludono il filtraggio persistente
- Confondono gli strumenti di analisi tarati su specifici tipi di attacco
- Forzano le difese a riavviare i cicli di mitigazione

Il risultato: perdite, esaurimento delle risorse e SOC fatica. Non si tratta di superare le difese, ma di stare un passo avanti.

Attacchi a Livello di Applicazione: Il DDoS è in Aumento

COSA DICONO I DATI

Le nostre osservazioni indicano costantemente un aumento degli attacchi di livello applicativo (Layer 7). Questi attacchi sono tipicamente:

- Larghezza di banda ridotta
- Più difficile da rilevare grazie alla crittografia
- API mirate, portali di login, carrelli della spesa, funzioni di ricerca e altri endpoint che richiedono molte risorse.

Abbiamo notato, sia internamente che nel settore, che le interruzioni delle applicazioni vengono sempre più spesso ricondotte ad attacchi di basso volume non visibili nei dati volumetrici tradizionali. Gli aggressori utilizzano anche le sonde L3/L4 come ricognizione per gli attacchi L7 successivi, rendendo ancora più confusa la linea di demarcazione tra le superfici di minaccia della rete e delle applicazioni.

Confronto tra attacchi DDoS L3/L4 e L7				
	Obiettivo	Tipo di Attacco	Sfida di Rilevamento	Focus sull'impatto
DDoS L3/L4	Infrastruttura di Rete	Alluvioni volumetriche	Velocità e volume dei pacchetti	Saturazione della Larghezza di Banda
DDoS L7	Applicazione e API	Imitare gli utenti legittimi	Comportamento/ Basato su modelli	Degradazione del Servizio

COSA SIGNIFICA

Il DDoS a livello di applicazione non consiste nell'allagare il tubo, ma nell'interrompere l'applicazione.

Questi attacchi possono:

Imitare il traffico degli utenti legittimi (ad es, richieste HTTPS GET/ POST)

Sfruttare l'esaurimento delle risorse (CPU/memoria/denaro) piuttosto che la larghezza di banda

Operare sotto il radar dei tradizionali strumenti di rilevamento volumetrico

Il passaggio a L7 riflette un'evoluzione più ampia: Il DDoS non è più incentrato solo sull'infrastruttura. È incentrato sul business. Gli aggressori di applicazioni mirano a distruggere chirurgicamente ciò che conta di più: l'esperienza del cliente, il flusso delle transazioni o l'autenticazione.

Questa tendenza sottolinea anche l'ascesa di avversari consapevoli delle piattaforme, che sanno come sfruttare le specifiche vittime. architetture, carichi di lavoro in cloud o logica delle applicazioni web-based.

Attacchi a Livello di Applicazione

COSA POTETE FARE

Iniziate a monitorare la salute del livello applicativo insieme al traffico di rete. Tempi di caricamento inusuali, errori 5xx o mancati accessi potrebbero essere un segnale di DDoS.

Integrate le funzionalità di difesa L7 nel vostro più ampio stack di mitigazione DDoS, anche se sono ancora in fase iniziale.

Collaborare con i team di sviluppo delle app e della piattaforma, non solo con le operazioni di rete, per sviluppare strategie di risposta coordinate.

Considerare la modellazione del comportamento dell'utente e le strategie di limitazione della velocità per rilevare l'abuso di firme ad alta velocità e a basso volume.

Quando il Traffico "Normale" Diventa un Attacco

Il DDoS a livello di applicazione è difficile da individuare perché spesso imita gli utenti reali. Un'inondazione di login può sembrare un lunedì di lavoro. Un attacco al carrello della spesa può sembrare il traffico del venerdì nero.

La differenza sta nell'intento e nello schema. Gli attacchi L7 sono tipicamente:

- Altamente ripetitivi
- Distribuiti su IP a rotazione
- Progettati per sprecare le risorse dell'applicazione piuttosto che quelle della rete

Per difendersi da ciò è necessaria un'analisi comportamentale e consapevolezza delle applicazioni, non solo filtraggio dei pacchetti.

I Difensori Stanno Ancora Recuperando Terreno

COSA DICONO I DATI

I difensori devono affrontare sfide sempre più impegnative per recuperare il ritardo accumulato, dato che i modelli di attacco DDoS sono diventati più automatizzati, adattivi ed evasivi. Secondo una ricerca commissionata da Corero e condotta da Merrill Research, una quota significativa di organizzazioni riferisce:

- Difficoltà di coordinamento tra i team di sicurezza, rete e piattaforma
- Impossibilità di mantenere una chiara visibilità su tutti i percorsi di traffico (soprattutto in ambienti ibridi e multi-cloud)
- Ritardi nei flussi di lavoro dal rilevamento alla mitigazione
- Carenza di personale qualificato per la gestione e la messa a punto delle difese di sicurezza

Questo rispecchia ciò che vediamo sul campo: i difensori non stanno fallendo a causa degli strumenti, ma stanno lottando a causa della loro capacità di gestire i problemi.

COSA SIGNIFICA

La postura difensiva è sempre più distribuita. L'adozione del cloud ha superato la visibilità. La linea di demarcazione tra i team che si occupano di applicazioni, infrastrutture e sicurezza è sfumata. E i playbook tradizionali presuppongono un livello di controllo che la maggior parte delle organizzazioni non ha più.

Anche i migliori sistemi di mitigazione sono validi solo quanto:

I segnali che ricevono

L'automazione che possono eseguire

La chiarezza della proprietà dietro di loro

Non tratta solo di un gap tecnologico. È una lacuna operativa.

I Difensori Stanno Ancora Recuperando Terreno

COSA POTETE FARE

- Conducete un audit di preparazione al DDoS, attraverso persone, processi e strumenti
- Chiarire la titolarità della risposta: chi gestisce il triage, chi recita, chi accorda?
- Creare playbook che riflettano la vostra infrastruttura reale, compresi i livelli ibrido, CDN e cloud.
- Investire nell'automazione, ma non dare per scontato che sia plug-and-play: necessita di visibilità e messa a punto.
- Rendere le esercitazioni DDoS da tavolo un evento regolare tra sicurezza e operazioni

La Risposta DDoS è un Gioco di Squadra

La risposta DDoS non è più affidata a un solo team. Tocca le operazioni di rete, i team delle applicazioni, gli architetti del cloud e gli analisti SOC. Eppure molte organizzazioni la trattano ancora come una disciplina isolata.

Per essere efficace, la mitigazione deve essere:

- Interfunzionale
- Pre-autorizzato
- Esercizio continuo

La vostra migliore difesa potrebbe non essere lo strumento più sofisticato: è la persone che sa quando e come.

Non è la Piattaforma. È la Pressione.

Finora ci siamo concentrati sul comportamento degli aggressori e sulle tendenze tecniche. Ma al centro di ognuna di queste intuizioni c'è una squadra umana incaricata di difendere in tempo reale, sotto pressione.

Ecco perché abbiamo incaricato Merrill Research di andare più a fondo. Volevamo capire non solo le minacce, ma anche come vengono vissute dagli operatori: i professionisti della sicurezza e delle reti che vivono la risposta, lo stress e la realtà della difesa sotto pressione.

Questi risultati riflettono i contributi dei clienti e dei non clienti Corero. L'obiettivo era semplice: capire cosa funziona, cosa non funziona e di cosa hanno bisogno i difensori.

La difesa DDoS non è una questione di funzionamento della tecnologia. Si tratta di capire se i team sono in grado di lavorare con essa. funzioni, in tempo reale e sotto pressione.

La ricerca Merrill ha messo in luce uno schema coerente: le sfide che i difensori devono affrontare non riguardano la capacità, ma il coordinamento. Anche con strumenti solidi, molti team faticano ad allinearsi tra piattaforme, ruoli e flussi di lavoro.

Temi chiave emersi:

Difficoltà a dimostrare il valore del DDoS protezione degli stakeholder aziendali

Coordinamento limitato tra i team di cloud, rete e applicazioni

Lacune nella messa a punto, nei manuali e nelle strategie di risposta integrate

Incertezza sulla proprietà e sulla comunicazione durante le minacce attive.

Il "quindi" è questo: la resilienza non viene dagli strumenti da solo. Viene dall'allineamento.

Quando i team sono in grado di vedere con chiarezza, agire con decisione e comunicare con sicurezza, non solo reagiscono più velocemente. Si riprendono più forti.

I fornitori hanno la responsabilità di ridurre l'onere operativo che impongono ai loro clienti, con prodotti che si integrano facilmente nelle architetture, nei flussi di lavoro e negli ecosistemi di strumenti esistenti e che possono essere integrati loro volta. Una buona tecnologia dovrebbe adattarsi al modo in cui i team già operano, non il contrario.

Cosa ci Hanno Detto i Difensori

68%
segnala che dimostrare il ROI della protezione DDoS alla leadership è una sfida.

51%
segnala che la mancanza di coordinamento tra i team rappresenta una vulnerabilità significativa.

47%
segnala difficoltà nell'adattare gli strumenti esistenti ad ambienti ibridi.

E più della metà dichiara di non essere fiduciosa nella propria capacità di mitigare gli attacchi avanzati senza la guida del fornitore.

Conclusione: Vedere il Segnale nel Rumore

Il panorama delle minacce DDoS nel 2024 non era caratterizzato dal caos. Era caratterizzato dalla chiarezza, per coloro che sapevano dove guardare.

Gli attacchi brevi e sub-saturanti hanno continuato a dominare il panorama, più frequenti che mai e tatticamente efficienti. All'altro estremo dello spettro, gli attacchi su larga scala hanno acquisito nuovo slancio, favoriti dalle moderne botnet e dai toolkit di base. E nel mezzo, un notevole calo degli attacchi di medie dimensioni ci ha detto qualcos'altro: gli aggressori stanno ottimizzando.

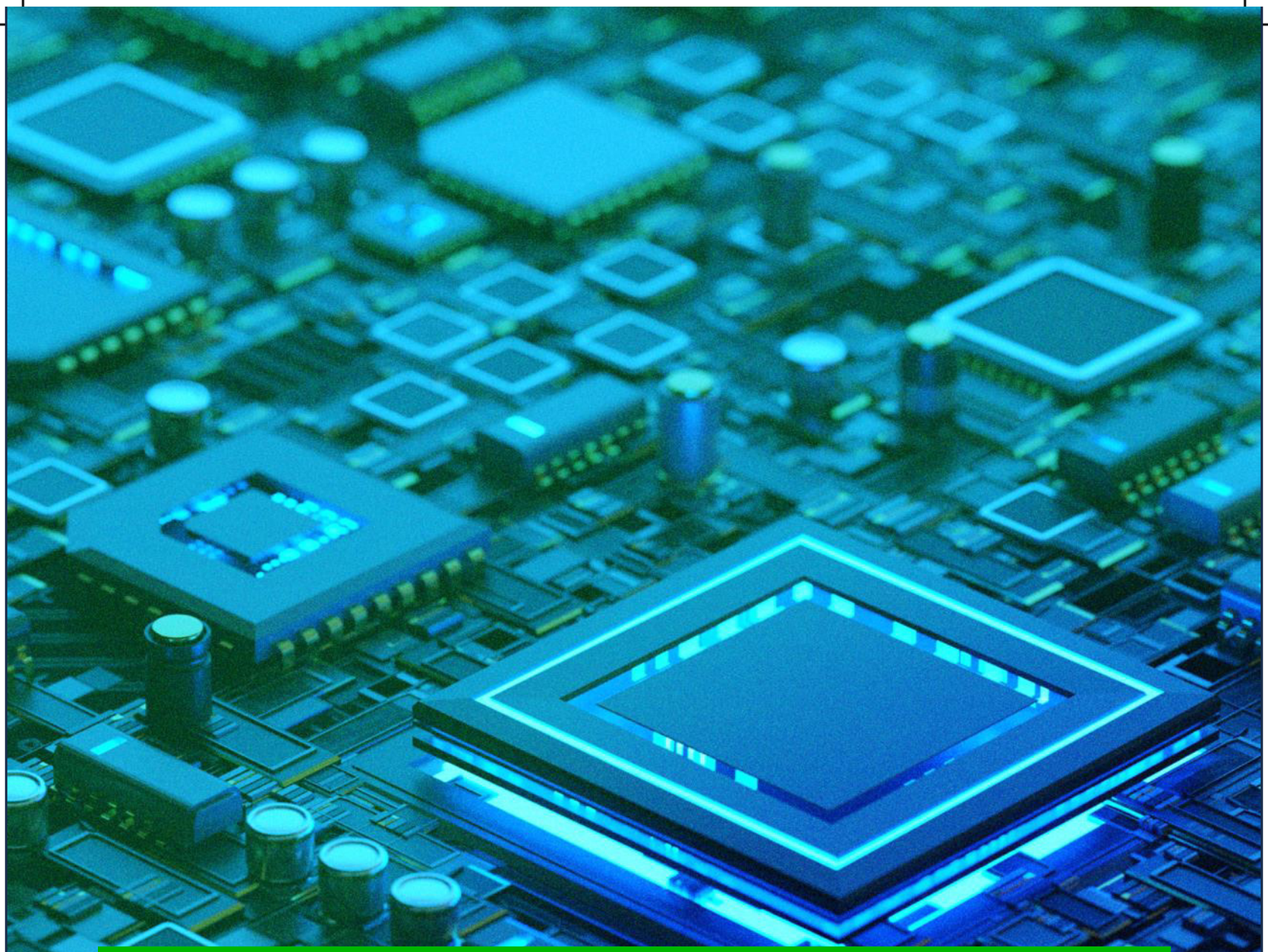
Scelgono i loro momenti. I loro metodi. I loro obiettivi.

Ma le tendenze tecniche raccontano solo una parte della storia. Con l'evoluzione dei dati, si è evoluta anche l'esperienza di difesa. La ricerca Merrill ha messo in luce ciò che molti già pensano: la sfida non è sempre la capacità. Si tratta di allineamento. Visibilità. Fiducia. Ed essere pronti quando l'attacco è reale, ma non ancora evidente.

Per difendersi dalle moderne campagne DDoS non bastano mitigazioni più rapide o filtri più intelligenti. Richiede l'integrazione di strumenti, persone e strategie. La postura più forte non si basa su una singola piattaforma. Si basa sul coordinamento, sulla chiarezza e su un supporto all'altezza della velocità della minaccia.

Il DDoS è facile. La difesa non lo è ancora. Ma quando i difensori sono allineati, informati e responsabilizzati, è allora che la il vantaggio inizia a spostarsi.

Il segnale 'è. **Anche la soluzione.**



corero
[NETWORK SECURITY]

INFORMAZIONI SU CORERO NETWORK SECURITY

Corero Network Security è un fornitore leader di soluzioni di protezione contro gli attacchi DDoS, specializzato in soluzioni automatiche di rilevamento e protezione, con strumenti di visibilità della rete, analisi e reportistica. La tecnologia di Corero protegge dalle minacce DDoS esterne e interne in ambienti complessi, sia di rete perimetrale che di sottoscrittori, garantendo la disponibilità del servizio Internet. Con centri operativi a Marlborough, Massachusetts (USA) e a Edimburgo (Regno Unito), Corero ha la sede centrale a Londra ed è quotata sul mercato AIM della Borsa di Londra (ticker: CNS) e sul mercato OTCQX degli Stati Uniti (OTCQX: DDOSF).

Per ulteriori informazioni, visitate il sito www.corero.com e seguiteci su LinkedIn e Twitter.