A10

Always Secure. Always Available.

MINACCIA CRESCENTE
Proteggere i Servizi Finanziari Italiani dagli Attacchi DDoS: la soluzione A10 basata sull'AI

Giacinto Spinillo
Sales Manager Italy & Benelux

Evento ABI «Banche & Sicurezza 2025» : Milano 27-28 Maggio 2025

Il Settore Finanziario: Un Obiettivo Privilegiato

Perché gli istituti finanziari sono bersagli preferiti?

Vasti archivi di dati personali identificabili (PII) e informazioni finanziarie sensibili

Potenziale per guadagni monetari significativi tramite furto d'identità o frode

Impatto sull'intero ecosistema finanziario europeo e globale

Interessi geopolitici e motivazioni politiche degli attori statali

Distribuzione degli attacchi DDoS

154%
Aumento degli attachi DDoS al settore finanziaro tra 2022 e 2023

66%
Degli attachi DDoS globali colpiscono istituzioni finanziarie nella regione EMEA

Gli attachi DDoS vengono spesso usati come “cortina di fumo” per mascherare altre attività malevole

Gli Attacchi DDoS nel Settore Finanziario Italiano

Perché gli attacchi DDoS sono così popolari?

Facilità di esecuzione

Servizi "DDoS-as-a-Service" nel dark web richiedono poche competenze tecniche per essere utilizzati

Potenziamento tramite IA

Strumenti di intelligenza artificiale consentono attacchi automatizzati più complessi e su larga scala

Attacchi usati come cortina di fumo

Il DDoS viene utilizzato per distrarre mentre si eseguono altri attacchi più mirati e dannosi

Caso di studio: Attacchi in Italia

Febbraio 2025

Ondata di attacchi DDoS contro istituzioni finanziarie italiane di alto profilo

Banche colpite

Intesa Sanpaolo, Banca Monte dei Paschi, Iccrea Banca

Gruppo responsabile

Attacco rivendicato dal gruppo hacker 'NoName057(16)' con apparenti motivazioni politiche

Impatto globale

Gli attacchi alle banche italiane possono influenzare l'intero ecosistema finanziario europeo e globale

Trend in crescita

Le ricerche mostrano un incremento del 154% negli attacchi DDoS contro le istituzioni finanziarie tra il 2022 e il 2023

Anatomia degli Attacchi DDoS

Tipologie di Attacchi DDoS

Attacchi Volumetrici

Sovraccaricano la larghezza di banda della rete con un enorme volume di traffico falso, saturando le risorse del server e rendendo inaccessibili i servizi legittimi.

Attachi di Protocollo

Mirano specificamente a sovrastare le risorse di sicurezza come firewall e load balancer, sfruttando vulnerabilità nei protocolli di rete.

Attachi a Livello Applicativo

Concentrano le risorse su specifiche funzionalità di un'applicazione web, richiedendo poche risorse per essere eseguiti ma causando danni significativi.

Come Funziona un Attacco DDoS

Rete di dispositivi compromessi (botnet)

Attaccante

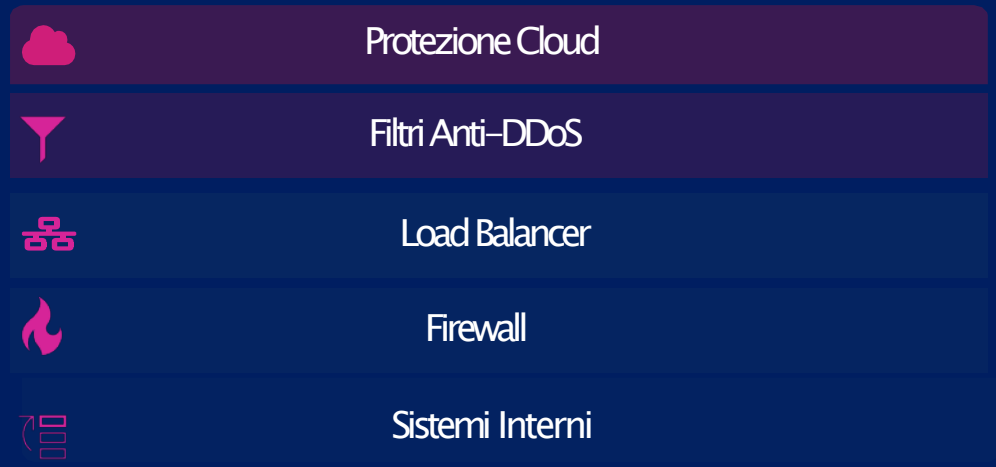
Server obiettivo

Perché è difficile fermare un attacco DDoS

- Il traffico proviene da migliaia di fonti diverse, rendendo impossibile bloccare un singolo IP
- Le richieste appaiono simili al traffico legittimo, complicando il filtraggio
- La scala degli attacchi può superare facilmente la capacità delle soluzioni di sicurezza tradizionali

Strategie di Protezione per il Settore Finanziario

Soluzione di Sicurezza Multi-livello



Una soluzione di sicurezza efficace deve proteggere contro ogni tipo di attacco DDoS: volumetrico, protocollo e applicativo.

Difesa Ibrida

Soluzioni On-Premise + Cloud

Un approccio ibrido assorbe e mitiga i picchi di traffico, impedendo che la rete interna venga sopraffatta durante attacchi di grandi dimensioni. Le soluzioni on-premise da sole non possono difendere contro attacchi che mirano a sopraffare la larghezza di banda del cloud

L'Intelligenza Artificiale come Soluzione

Analisi del Traffico

Identifica modelli sospetti in tempo reale con maggiore efficienza

Apprendimento Continuo

Si adatta ai nuovi vettori d'attacco e alle minacce emergenti

Analisi Comportamentale

Riconosce anomalie nei pattern di utilizzo degli utenti

Baseline del Traffico

Stabilisce parametri normali per identificare deviazioni sospette

Sfide per la Sicurezza Finanziaria

Conformità Normativa

Le istituzioni finanziarie devono conciliare la sicurezza informatica con le normative europee e italiane, affrontando al contempo la crescente complessità tecnologica delle loro infrastrutture.

Implementare un Piano di Risposta agli Attacchi DDoS

Ciclo di Risposta agli Incidenti

Matrice di Responsabilità

Fase	IT Security	Network Ops	Management
Rilevamento Iniziale	Primario	Supporto	—
Classificazione Attacco	Primario	Supporto	Informato
Mitigazione	Supporto	Primario	Informato
Comunicazione Esterna	—	—	Primario

Elementi Chiave del Piano

Team di Risposta
Designare un team dedicato con ruoli e responsabilità chiaramente definiti

Monitoraggio Continuo
Implementare sistemi di monitoraggio 24/7 con soglie di allerta predefinite

Fornitori Esterni
Stabilire accordi con provider di mitigazione DDoS specializzati

Comunicazione
Definire protocolli di comunicazione interna ed esterna durante un attacco

Consigli per Banche Italiane

- Condurre esercitazioni periodiche di simulazione di attacchi DDoS
- Partecipare a gruppi di condivisione di informazioni come FS-ISAC
- Implementare sistemi di backup per servizi critici
- Mantenere aggiornati i piani di continuità operativa

Il Futuro della Protezione DDoS per il Settore Finanziario

Tendenze Emergenti

IA Avanzata per Difesa e Attacco

L'intelligenza artificiale sarà utilizzata sia dagli attaccanti per orchestrare attacchi più sofisticati, sia dalle istituzioni finanziarie per implementare sistemi difensivi predittivi e auto-adattativi.

Soluzioni Zero-Trust

Adozione di architetture di sicurezza che non concedono fiducia predefinita, richiedendo sempre verifiche, anche per il traffico interno, mitigando così i vettori d'attacco potenziali.

Sicurezza DevSecOps

Integrazione della sicurezza nell'intero ciclo di sviluppo delle applicazioni finanziarie, costruendo resilienza agli attacchi DDoS direttamente nel codice.

Valutazione della Preparazione DDoS

Azioni Prioritarie per Istituzioni Finanziarie Italiane

Collaborazione di Settore

Partecipare attivamente alla condivisione di intelligence sulle minacce tramite consorzi come FS- ISAC e CERTFin

Investimenti Tecnologici

Adottare soluzioni di sicurezza di nuova generazione con capacità analitiche avanzate e machine learning

Formazione Continua

Aggiornare regolarmente le competenze dei team di sicurezza sulle nuove tecniche di attacco e difesa

Resilienza Distribuita

Creare architetture multi-cloud e multi-regione per garantire la continuità operativa anche durante attacchi massivi

Benchmark del Settore Finanziario Italiano vs UE

Investimenti in Cybersecurity	Preparazione DDoS	Adozione Cloud Sicuro	Condivisione Intelligence
70%	65%	60%	75%

Conclusioni e Prossimi Passi

Punti Chiave

- Il settore finanziario italiano affronta una minaccia DDoS crescente con impatti potenzialmente sistemici
- Le soluzioni di sicurezza devono essere multi-livello per contrastare tutti i tipi di attacchi DDoS
- L'intelligenza artificiale rappresenta sia una sfida sia un'opportunità per la sicurezza del settore
- La collaborazione tra istituti finanziari è fondamentale per rafforzare la resilienza dell'intero settore

Prossime Azioni Raccomandate

1. Condurre una valutazione completa della propria capacità di difesa contro gli attacchi DDoS
2. Implementare soluzioni difensive ibride cloud/on-premise
3. Investire in tecnologie basate su AI per rilevamento e mitigazione
4. Sviluppare e testare regolarmente un piano di risposta agli incidenti DDoS

Il Costo dell'Inazione

Perdite Finanziarie

Gli attacchi DDoS possono costare alle istituzioni finanziarie fino a 100.000€ all'ora in mancati ricavi e costi operativi

Danno Reputazionale

La fiducia dei clienti può essere compromessa in modo significativo, con effetti a lungo termine difficili da quantificare

Rischi Normativi

Le autorità di regolamentazione stanno intensificando le richieste di resilienza operativa per le istituzioni finanziarie

Inizia Oggi il Tuo Percorso verso la Sicurezza

Richiedi una Valutazione della Sicurezza

Giacinto Spinillo
gspinillo@a10networks.com
+39 335 7483344
https://www.a10networks.com/

A10

Always Secure. Always Available.

Thank You

- Giacinto Spinillo – Mob. 335 7483344
- Email: gspinillo@a10networks.com