Attacchi DoS: Identificazione, Analisi e Mitigazione

Un attacco Denial of Service (DoS) rappresenta una minaccia significativa per la continuità operativa aziendale. Quando i server vengono inondati da un volume anomalo di richieste, i servizi web diventano inaccessibili agli utenti legittimi, causando interruzioni che possono avere conseguenze gravi.

In questa presentazione, esploreremo le caratteristiche degli attacchi DoS/DDoS, analizzeremo i rischi associati, e delineeremo strategie efficaci per identificare, mitigare e prevenire questi attacchi.

Cos'è un Attacco DoS/DDoS

Denial of Service (DoS)

Mira a rendere una risorsa di rete non disponibile agli utenti legittimi attraverso un'inondazione di richieste da una singola fonte.

Distributed Denial of Service (DDoS)

Un attacco DoS lanciato da molteplici sistemi compromessi (botnet) contemporaneamente, più potente e difficile da mitigare.

Obiettivo Primario

Interrompere il servizio impedendo agli utenti legittimi di accedere a siti web, applicazioni o altri servizi online offerti dall'azienda.

Gli attacchi DoS/DDoS rappresentano una minaccia significativa alla disponibilità dei servizi digitali. La differenza principale tra DoS e DDoS sta nella distribuzione dell'attacco: mentre il primo proviene da una singola fonte, il secondo utilizza una rete di dispositivi compromessi per amplificare l'impatto.

Tipologie di Attacchi DoS/DDoS

Attacchi Volumetrici

Inondano la rete con un'enorme quantità di traffico (es. UDP flood, ICMP flood) per saturare la banda disponibile.

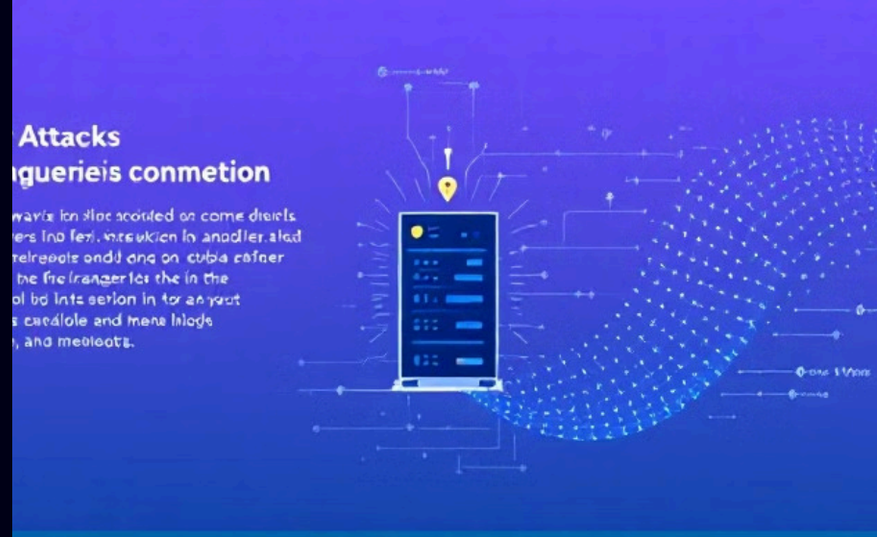
Attacchi a Protocollo

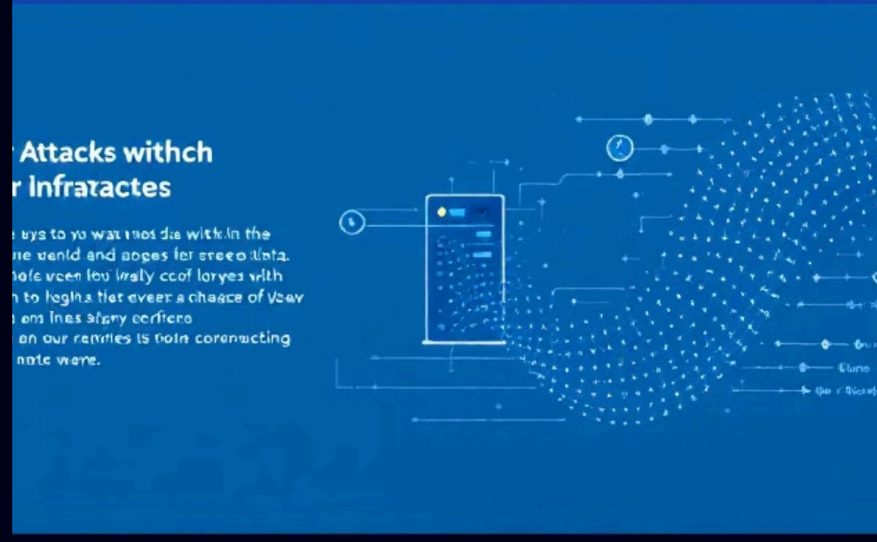
Sfruttano debolezze nei protocolli di rete (es. SYN flood, Ping of Death) per consumare le risorse dei server o dei dispositivi di rete intermedi.

Attacchi a Livello Applicativo

Inviano richieste apparentemente legittime ma create ad arte per sovraccaricare specifiche risorse dell'applicazione o del server web (es. HTTP flood, Slowloris attack).

Ogni tipologia di attacco DoS/DDoS utilizza tecniche diverse per raggiungere lo stesso obiettivo: rendere un servizio inaccessibile. La comprensione del tipo specifico di attacco è fondamentale per implementare le contromisure più efficaci.





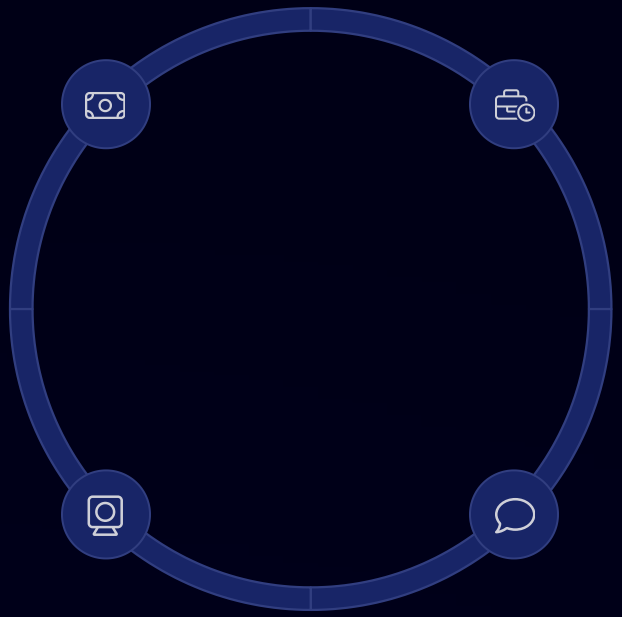
Analisi del Rischio

Perdita di Entrate

Particolarmente grave per e-commerce o servizi a pagamento che dipendono dalla disponibilità continua.

Distrazione Strategica

Potenziale copertura per altri tipi di attacchi più mirati mentre il team IT è concentrato sul DoS.



Interruzione Operativa

Può paralizzare le operazioni aziendali se colpisce applicazioni interne critiche.

Danno Reputazionale

Erosione della fiducia dei clienti dovuta alla percepita inaffidabilità dei servizi.

L'impatto potenziale di un attacco DoS/DDoS è classificato come Medio-Alto, con conseguenze che si estendono ben oltre la semplice indisponibilità temporanea. I servizi critici maggiormente a rischio includono siti web pubblici, piattaforme di e-commerce, API, servizi VPN, applicazioni web interne e server DNS aziendali.

Rilevamento e Analisi

Rilevare l'Attacco

Utilizzare sistemi di monitoraggio di rete (traffico, latenza, errori server), alert da firewall/IDS/IPS e raccogliere segnalazioni dagli utenti per identificare rapidamente un potenziale attacco in corso.

Identificare le Caratteristiche

Analizzare i log (firewall, server web, router) per determinare il tipo di attacco, le porte/protocolli target, e, se possibile, le fonti del traffico. Strumenti come NetFlow/sFlow sono fondamentali.

Valutare l'Impatto

Determinare quali servizi sono affetti e la gravità dell'interruzione per prioritizzare gli interventi e allocare le risorse in modo efficiente.

La fase di rilevamento e analisi è cruciale per una risposta efficace. Un'identificazione tempestiva delle caratteristiche dell'attacco consente di implementare contromisure mirate, riducendo il tempo di inattività e limitando l'impatto complessivo sull'organizzazione.

Mitigazione del Traffico Malevolo

Attivare Difese Pre-esistenti

Se disponibili, attivare immediatamente servizi di mitigazione DDoS (basati su cloud o on-premise) configurati in precedenza.

Filtrare il Traffico

Implementare regole di filtraggio sui firewall perimetrali o router: bloccare IP sorgente specifici, applicare rate limiting, utilizzare tecniche come SYN cookies contro SYN flood.

Contattare l'ISP

Informare il proprio Internet Service Provider che potrebbe essere in grado di applicare filtri a monte ("upstream filtering") o aiutare a identificare/bloccare il traffico malevolo.

Null Routing (Blackholing)

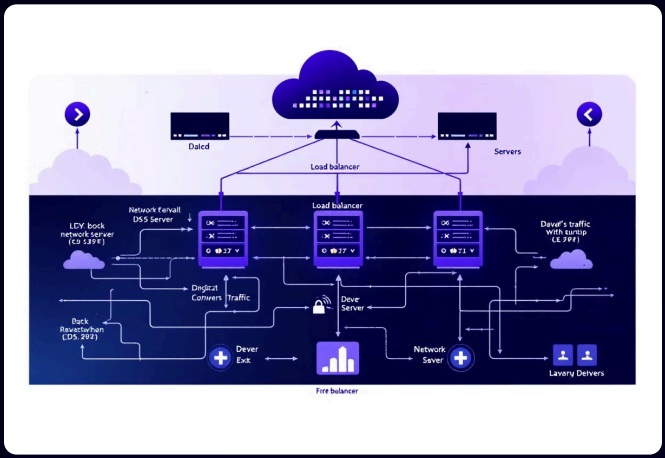
Come ultima risorsa, richiedere all'ISP di reindirizzare tutto il traffico verso l'IP target nel "nulla" per proteggere il resto dell'infrastruttura.

La mitigazione efficace richiede un approccio stratificato che combini diverse tecniche. La scelta delle contromisure dipende dalla natura e dall'intensità dell'attacco, nonché dalle risorse disponibili all'organizzazione.

Implementazione della Remediation

Bilanciamento del Carico

I load balancer possono distribuire il carico su più server e alcuni offrono funzionalità base di rate limiting o blocco IP. Possono rimuovere rapidamente un server sovraccarico dalla rotazione.



Servizi di Mitigazione DoS

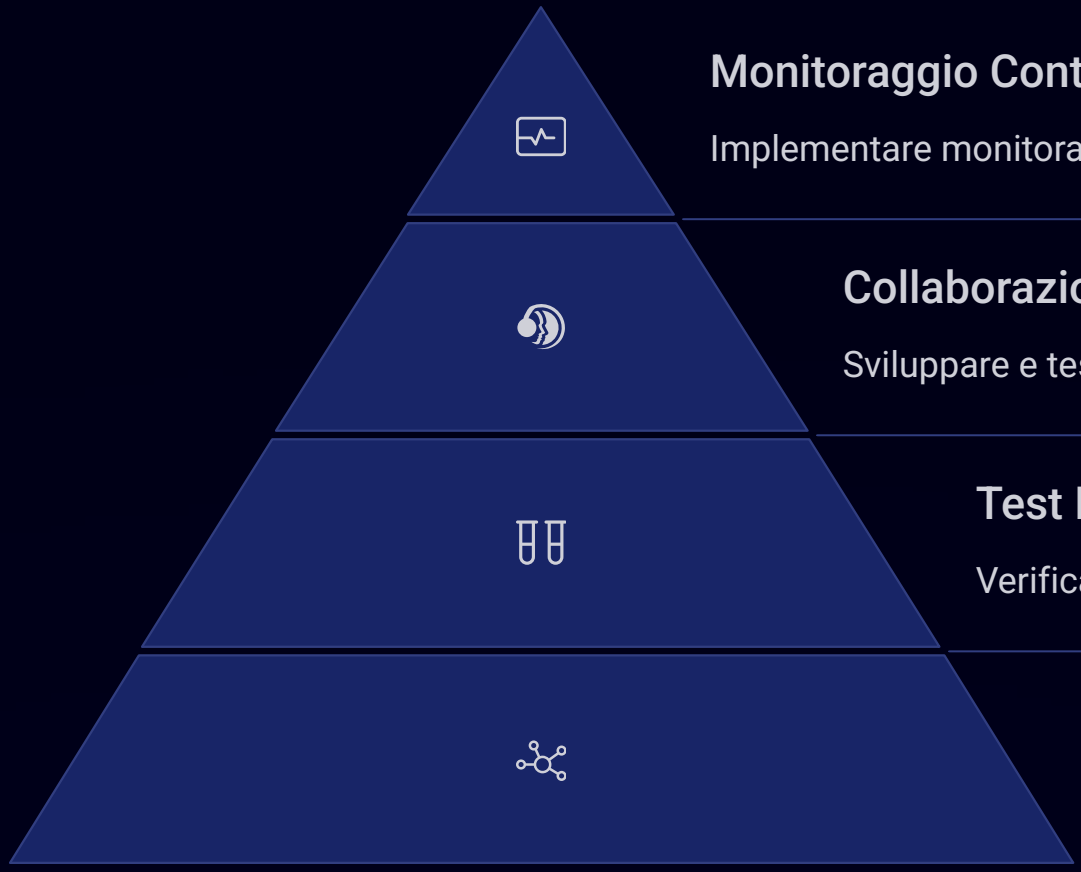
Attivare o scalare servizi dedicati (es. Cloudflare, Akamai, AWS Shield, Azure DDoS Protection) che "puliscono" il traffico prima che raggiunga la rete aziendale, assorbendo gli attacchi volumetrici e filtrando quelli a livello di protocollo e applicativo.

Questa è spesso la misura più efficace contro attacchi su larga scala.

Configurazione Firewall/Router

Applicare regole di filtraggio e rate limiting identificate nel piano. Assicurarsi che i dispositivi di rete siano configurati in modo sicuro (hardening) per resistere essi stessi agli attacchi.

Prevenzione e Preparazione Futura



Monitoraggio Continuo

Implementare monitoraggio 24/7 con alert automatici

Collaborazione e Preparazione

Sviluppare e testare piani di risposta

Test Periodici di Resilienza

Verificare l'efficacia delle difese

Architettura di Rete Resiliente

Garantire ridondanza e capacità adeguata

La prevenzione efficace richiede un approccio proattivo che combini monitoraggio continuo, preparazione del team, test regolari e un'architettura di rete progettata per la resilienza. Stabilire rapporti e procedure chiare con l'ISP e con provider di servizi di mitigazione DDoS prima che un attacco si verifichi è fondamentale per una risposta rapida ed efficace.