Attacchi Ddos

Gli attacchi Distributed Denial of Service, tradotto “Interruzione distribuita del servizio” (DDos), sono una forma di attacco informatico che coinvolge tipicamente un gran numero di dispositivi infettati da malware (una botnet) e distribuiti geograficamente che inviano un volume eccessivo di richieste o traffico alla vittima, il cui scopo è quello di rendere inaccessibile un server, un sito web oppure un servizio online sovraccaricandone la rete.

Per capire cos’è un attacco DDoS, bisogna prima comprenderne la versione meno sofisticata: il DoS, cioè Denial of Service.
Un’azione il cui obiettivo è quello di ingolfare le risorse di un sistema informatico che fornisce un determinato servizio ai computer connessi, prendendo di mira server, reti di distribuzione, o data center che vengono inondati di false richieste di accesso, a cui non riescono a far fronte.
In gergo si dice che ne viene saturata la banda di comunicazione e i siti web o i naviganti che cercano di raggiungere quella determinata risorsa online hanno difficoltà, o non ci riescono del tutto.
Gli attacchi DDos invece funzionano allo stesso modo, ma avvengono su scala molto più ampia, quindi utilizzando una botnet.
Nei casi di Dos, infatti, bisogna difendersi da una sola fonte di traffico informatico: per esempio, un numero elevato di email in arrivo contemporaneamente. Mentre durante gli attacchi DDoS le domande fasulle arrivano nello stesso momento da più fonti, determinando così una maggiore efficacia dello strumento che per funzionare ha bisogno di minor tempo creando effetti disastrosi che durano anche più a lungo: si può parlare di diverse ore come di diversi giorni, in base alla prontezza di reazione all’attacco.

Gli obiettivi significativi degli attacchi ddos e in cosa si contraddistinguono:

1. Disponibilità dei servizi: Il principale obiettivo è rendere un sito web o un servizio online non disponibile, danneggiandone la reputazione e causando perdite finanziarie.
2. Distrazione: Gli attacchi DDoS possono essere utilizzati come diversivo per coprire altri attacchi mirati, come intrusioni o furti di dati.
3. Estorsione: Gli attaccanti possono minacciare di eseguire un attacco DDoS a meno che non venga pagato un riscatto.

Esempi di tecniche utilizzate negli attacchi DDoS

1. Attacchi di sovraccarico della CPU: Gli attaccanti inviano richieste complesse che richiedono molta elaborazione da parte del server, portandolo al collasso.
2. Attacchi di sovraccarico dell'applicazione: Gli attaccanti mirano alle vulnerabilità delle applicazioni web per sovraccaricare i server con richieste legittime.
3. Amplificazione: Gli attaccanti sfruttano server o dispositivi aperti su Internet per amplificare il traffico in uscita, aumentando l'efficacia dell'attacco.
4. Attacchi di sovraccarico della larghezza di banda: Gli attaccanti inviano un volume massiccio di dati alla vittima per saturarne la larghezza di banda e impedirne l'accesso.

A seconda dei metodi utilizzati e degli obiettivi che si propongono, gli attacchi DDoS possono essere raggruppati in quattro principali categorie. Ci sono quelli che prendono di mira la connessione TCP, puntando tutto sulla velocità. In questo caso, la botnet inonda il server di richieste di connessione,

senza mai arrivare alla fine: così la banda di comunicazione del sistema informatico viene saturata in fretta, rendendo impossibile l'accesso ai contenuti da parte di qualunque utente.
Un'altra tipologia di DDoS sono gli attacchi volumetrici in cui il volume di traffico creato è enorme e diventa ingestibile.
Tutt'altro discorso, invece, per gli attacchi di frammentazione che ambiscono a consumare le risorse di calcolo del sistema informatico inviando richieste d'accesso incomplete. Come conseguenza l'oggetto dell'attacco usa gran parte delle proprie risorse per tentare di ricostruire l'informazione digitale ricevuta. Infine, ci sono gli attacchi applicativi che non puntano all'intera infrastruttura, bersagliando un programma indispensabile, rendendolo instabile e inutilizzabile.

I cybercriminali sembrano aver accantonato attacchi prolungati, preferendo attacchi frequenti e veloci: DDoS "mordi e fuggi", che vengono interrotti dopo pochi minuti. In questo modo, le aziende colpite non hanno neanche il tempo di riprendersi prima di far fronte a una nuova minaccia.

Quali sono le conseguenze degli Attacchi DDoS

Questi tipi di attacco possono causare gravi conseguenze, tra cui:

1. Interruzione dei servizi: L'obiettivo principale è rendere inaccessibile un servizio, danneggiandone la reputazione e causando perdite finanziarie.
2. Perdita di dati: In alcuni casi, gli attacchi DDoS possono essere utilizzati come diversivo per ulteriori attacchi, come intrusioni e furti di dati.
3. Danno alla reputazione: Un servizio o un'azienda che subisce frequenti attacchi DDoS può perdere la fiducia dei clienti e subire danni reputazionali.

Alcuni esempi di attachi Ddos nella storia:

Attacco Ddos contro AWS (Amazon Web Services)

ha segnalato la mitigazione di un massiccio attacco DDoS a febbraio 2020. Al culmine dell'attacco venne registrato traffico in entrata a una velocità di 2,3 terabit al secondo (Tbps).
Gli aggressori responsabili utilizzavano server Web CLDAP (Connection-less Lightweight Directory Access Protocol) compromessi. CLDAP è un protocollo per le directory utente alternativo a LDAP, la vecchia versione.

Attacco DDoS contro GitHub: Nel 2018, GitHub è stato colpito da un enorme attacco DDoS che ha superato i 1,3 terabit al secondo di traffico. Gli attaccanti hanno sfruttato il protocollo di amplificazione Memcached per intensificare l'attacco. Successivamente GitHub è riuscito a mitigare l'attacco con successo.

Attacco DDoS contro Dyn: Nel 2016, Dyn, un importante fornitore di servizi DNS, è stato oggetto di un attacco DDoS massiccio. Questo attacco ha influenzato l'accesso a numerosi servizi online, tra cui Twitter, Reddit, Netflix e Amazon. La botnet utilizzata per l'attacco era composta principalmente da dispositivi IoT infettati, sottolineando la crescente minaccia di sicurezza legata a questi dispositivi.

Attacco DDoS all'Arabia Saudita: Nel 2012, l'Arabia Saudita è stata soggetta a una serie di attacchi DDoS su siti web governativi e finanziari. Gli attacchi, che sono stati attribuiti a un gruppo hacker chiamato "The Izz ad-Din al-Qassam Cyber Fighters," sono stati condotti in risposta a un video

offensivo su YouTube. Questi attacchi sono stati noti per l'uso di botnet e hanno dimostrato come gli attacchi DDoS potessero avere motivazioni politiche o ideologiche.

Attacco DDoS al sito web della Casa Bianca: Nel 2014, il sito web della Casa Bianca è stato soggetto a un attacco DDoS. Sebbene il sito non sia stato gravemente danneggiato, l'attacco ha sollevato preoccupazioni sulla sicurezza delle infrastrutture governative.

Quali sono le misure di Difesa contro Attacchi DDoS

1. Firewall e filtro del traffico: Utilizzare soluzioni di filtraggio del traffico per bloccare il traffico sospetto o indesiderato.
2. Bilanciatori di carico: Distribuire il traffico su più server per mitigare gli attacchi.
3. Servizi di mitigazione DDoS: Sottoscrivere servizi di mitigazione DDoS da fornitori specializzati.
4. Monitoraggio e rilevamento: Monitorare costantemente il traffico per rilevare attacchi in corso.
5. Pianificazione per la resilienza: Implementare strategie di pianificazione e ripristino per mitigare gli impatti degli attacchi.

Difendersi è molto difficile ed è meglio poter attrezzarsi prima di essere attaccati.
Una possibile contromossa rispetto agli attacchi applicativi è un'infrastruttura scalabile e resiliente (cluster di front-end web, database, firewall, e così via).
Dai DDoS di banda, invece, si può essere protetti solo dai provider dei servizi internet (ISP).
Esistono, poi, gli attacchi mirati particolarmente complessi che vanno gestiti di volta in volta.

Conoscere l'infrastruttura e i suoi punti deboli. Quali sono i servizi che garantiscono la stabilità e il funzionamento della vostra organizzazione? Pensare anche ai sistemi base essenziali per il funzionamento dei programmi aziendali;

Conoscere lo «stato normale» delle reti e dei sistemi ed essere in grado di rilevare le anomalie (ad es. con sistemi IDS per la valutazione centralizzata dei log). Un attacco DDoS andrebbe scoperto prima che lo notino i clienti.

Controllare la disponibilità delle applicazioni clienti anche dal punto di vista dei clienti, ossia tramite il collegamento Internet;

Ottimizzazione dei sistemi (senza servizi inutili, assegnazione controllata dei diritti, elevato livello di autenticazione), aggiornamenti delle patch

un firewall permette di accedere al sistema solo ai protocolli necessari. Il firewall dispone di risorse di sistema sufficienti per continuare a funzionare anche in caso di attacco DDoS. Occorre prestare particolare attenzione alla «connection table» e a una buona gestione delle regole che permettano di implementare ulteriori regole di blocco in caso di emergenza;

Verificare le possibilità di impostare un blocco su base GeoIP. Se i clienti provengono principalmente dalla Svizzera o dai Paesi vicini, è possibile creare un profilo che dia la priorità agli indirizzi di quest'area o che blocchi altri indirizzi IP. In caso di attacco è possibile attivare questo profilo, ottenendo così rapidamente nuove possibilità di intervento e una maggiore protezione.

Predisporre soluzioni alternative, ad esempio creando su un altro provider un sito Internet statico con un minimo indispensabile di informazioni che possa essere attivato con una semplice modifica del DNS.

Bilanciare i TTL del server DNS in modo da poter contrastare tempestivamente un tentativo di identificare l'indirizzo IP del dominio.

Mettere a punto una strategia da attuare in caso di attacco DDoS. I responsabili devono conoscere la procedura e i contatti interni ed esterni (service provider, polizia ecc.);

Discutete degli attacchi DDoS a livello aziendale e con i partner esterni e effettuate delle simulazioni. Così in caso di attacco ognuno sa qual è il suo ruolo e a chi rivolgersi.

Conclusioni

Gli attacchi DDoS rappresentano una minaccia significativa per l'accessibilità e la sicurezza dei servizi online. La consapevolezza, la preparazione e l'implementazione di misure di difesa adeguate sono essenziali per proteggere le infrastrutture digitali da tali attacchi. La collaborazione tra organizzazioni e fornitori di servizi può contribuire a una mitigazione più efficace degli attacchi DDoS.

Giovanni Saponaro