Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Organo direzione informatica della Confederazione ODIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
GovCERT.ch

Misure contro attacchi DDoS

MELANI / GovCERT.ch

Versione:	v1.00
Autore:	MELANI / GovCERT.ch

Disclaimer: tutti i loghi utilizzati in questo documento sono marchi registrati e/o di proprietà dei relativi titolari. La presente guida può essere modificata secondo le condizioni Creative Commons (CC BY-ND 3.0[1]).

[1] http://creativecommons.org/licenses/by-nd/3.0/

Introduzione

L'acronimo DDoS («Distributed Denial of Service» = negazione del servizio) indica un attacco a sistemi informatici con lo scopo dichiarato di limitarne la disponibilità. Le conseguenze economiche per la vittima possono essere notevoli. A differenza di quanto avviene nel caso di un DoS semplice, l'attacco parte da più computer e può avvenire a livello di rete, di applicazione o di una combinazione di entrambi. Normalmente per questi attacchi si impiegano delle cosiddette «reti bot» (o «botnet»: un numero consistente di sistemi infettati che possono essere comandati a distanza dagli aggressori) o sistemi con errori di configurazione (ad esempio Open DNS Resolver) che vengono indotti, da richieste manipolate, ad inviare risposte voluminose all'indirizzo "sbagliato" – cioè quello del bersaglio (si parla di attacco di amplificazione). Il volume dei dati raggiunge spesso molte centinaia di Gbit/s. Si tratta di volumi che una singola organizzazione non riesce solitamente a fronteggiare senza un aiuto esterno. Anche firewall e IPS («intrusion prevention systems») appositamente configurati hanno un'efficacia solo limitata.
I motivi alla base degli attacchi DDoS sono per lo più legati all'attivismo politico, a tentativi di estorsione o all'intenzione di danneggiare un concorrente. Attualmente MELANI constata un aumento degli attacchi DDoS a fini di estorsione, nei quali viene richiesto un riscatto in criptovalute come Bitcoin o Litecoin.

DDoS può colpire qualsiasi organizzazione!

Misure preventive

In linea di massima tutti siamo già stati confrontati con la problematica dei DDoS e siamo pronti a difenderci:

- conoscete la vostra infrastruttura e i suoi punti deboli. Avete individuato i servizi che garantiscono la stabilità e il funzionamento della vostra organizzazione. In questo contesto tenete in considerazione anche i sistemi base essenziali per il funzionamento dei programmi aziendali;
- conoscete lo «stato normale» delle vostre reti e dei vostri sistemi e siete in grado di rilevare le anomalie (IDS, «intrusion detection system»: valutazione centralizzata dei log). Un attacco DDoS dovrebbe essere scoperto prima che lo notino i clienti;
- controllate la disponibilità delle applicazioni clienti anche dal punto di vista dei clienti, cioè tramite il collegamento Internet;
- i vostri sistemi sono ottimizzati (senza servizi inutili, assegnazione controllata dei diritti, elevato livello di autenticazione ecc.) e i patch sono aggiornati. I cookies SYN sono attivati ecc;
- l'introduzione di un firewall permette un accesso al sistema che si limita 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;
- verificate 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 predefinito 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;
- un «web application firewall» riduce al minimo le possibilità di attacco a servizi su base web;
- i sistemi che potrebbero diventare bersaglio di un attacco DDoS (p. es. il sito Internet) dovrebbero basarsi su un uplink Internet diverso rispetto agli altri sistemi dell'organizzazione. In questo modo è possibile proteggere più facilmente i sistemi interessati con un provider di mitigazione dagli attacchi DDoS senza ripercussioni sugli altri sistemi necessari per l'attività quotidiana;

- predisponete 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;
- in generale, cercate di bilanciare i TTL del server DNS in modo da poter contrastare tempestivamente un tentativo di indentificare l'indirizzo IP del dominio;
- mettete a punto una strategia da attuare in caso di attacco DDoS. I responsabili conoscono la procedura e i contatti interni ed esterni (service provider, polizia ecc.);
- nel peggiore dei casi potete ricorrere a risorse interne o esterne garantite su base contrattuale (in particolare, personale e infrastruttura);
- avete discusso degli attacchi DDoS a livello aziendale e con i partner esterni e sono state fatte delle simulazioni. Ognuno sa qual è il suo ruolo e a chi rivolgersi.

Contromisure in caso di attacco

In caso di attacco DDoS è fondamentale segnalare all'aggressore che non sta raggiungendo il suo obiettivo. Se la resistenza dura abbastanza a lungo, l'aggressore tende generalmente a desistere.

1. Documentate l'attacco (flussi di rete, log al server, corrispondenza e-mail con i ricattatori ecc.). Questi dati sono importanti per un'analisi successiva e un'eventuale denuncia.
2. Assicuratevi di poter tenere aperti determinati canali d’informazione verso l'esterno, per es. un sito Internet statico sul quale informare i clienti e indicare loro possibilità di contatto alternative (per es. telefono, fax, e-mail).
3. Analizzate l'attacco e stabilite una strategia di difesa:

    a. se l'attacco è partito da un numero limitato di indirizzi IP, può bastare un filtro per questi indirizzi nel router o nel firewall. Se il volume dei dati supera l'ampiezza della banda che avete a disposizione se ne deve occupare l'ISP;
    b. eventualmente spostate il sistema soggetto all'attacco su un'altra sottorete (nel caso di attacchi basati solo su IP). In questi casi conviene cercare una soluzione in stretta collaborazione con l'ISP e/o con un provider specializzato nella mitigazione di attacchi DDoS;
    c. se si tratta di un attacco in cui gli indirizzi IP sorgente sono stati probabilmente falsificati: questo accade solitamente nel caso di attacchi di tipo «SYN flooding», «UDP flooding», «BGP flooding» e «SNMP flooding». Filtrare gli indirizzi IP non ha senso, poiché si potrebbero addirittura bloccare degli utenti legittimi. Anche in questo caso la soluzione deve essere trovata in collaborazione con l'ISP, che può deviare e filtrare il traffico. A questo fine dovreste però sapere prima quali protocolli vengono utilizzati presso la vostra organizzazione e quali possono essere filtrati senza provocare danni. I siti accessibili al pubblico si limitano solitamente a protocolli su base TCP (HTTP, HTTPS, SMTP ecc.), quindi i protocolli «stateless» come UDP possono essere bloccati senza problemi con un filtro (eventuale eccezione: DNS);
    d. attacco a un’applicazione: in questo caso l'applicazione viene resa inutilizzabile da un gran numero di richieste (complesse). Di solito gli attacchi impiegano il protocollo di rete TCP. L'indirizzo di origine è quindi difficile da falsificare e può essere bloccato in base a diversi criteri di filtraggio;
    e. attacchi al protocollo SSL/TLS: può essere utile interrompere la connessione SSL a un servizio cloud che inoltra poi la connessione filtrata ai vostri sistemi;
    f. se la maggior parte della clientela si trova in determinati Paesi si può anche applicare un filtro GeoIP per concedere priorità o filtrare. In questo modo il servizio rimane disponibile il più a lungo possibile, anche se può succedere che alcuni utenti legittimi vengano bloccati o ricevano una priorità inferiore.

4. Siate preparati al fatto che gli aggressori tenteranno di reagire alle misure di difesa implementate ricorrendo a nuove tattiche. In questi casi analizzate nuovamente il DDoS e adottate contromisure corrispondenti.
5. Segnalate il caso a MELANI e presentate denuncia presso il posto di Polizia competente per (tentato) danneggiamento di dati (Art. 144 bis del Codice penale) e, qualora si sia verificata, per (tentata) estorsione (Art. 156 del Codice penale). Si parla di danneggiamento di dati anche nel caso in cui, a causa di un attacco, per un certo lasso di tempo, i dati non siano più fruibili e risultino perciò inutilizzabili.
6. MELANI sconsiglia vivamente di cedere alle richieste dei ricattatori.

Contatto MELANI

http://www.melani.admin.ch