Attacchi DDoS sempre più imponenti: l’era del terabit

Author : Redazione

Date : 14 settembre 2018

Da tempo, gli esperti di sicurezza informatica assistono con apprensione alla diffusione di attacchi DDoS di crescente volume e frequenza. A fronte di migliaia di attacchi sferrati continuamente in ogni parte del mondo, le grandi organizzazioni hanno dovuto rafforzare le proprie difese contro eventi che, in molti casi, possono anche assumere una frequenza quotidiana. Nell’ultimo **NETSCOUT Threat Intelligence Report**, i nostri ricercatori hanno spiegato che la frequenza degli attacchi è in realtà diminuita tra il 2017 e il 2018. Tuttavia, il senso di sollievo che questa notizia potrebbe portare ai team di sicurezza bersagliati dagli attacchi è rapidamente cancellato da un altro trend allarmante: gli attacchi sono sì meno frequenti, ma si stanno moltiplicando per grandezza e riescono spesso a superare ampiamente i livelli di capacità difensiva considerati sicuri dai service provider. Questo avviene perché gli attacchi DDoS sono ormai entrati nell’era del terabit.

Secondo il team ASERT (ATLAS Security Engineering and Response Team) di NETSCOUT, le dimensioni massime degli attacchi DDoS sono aumentate del 174% nella prima metà del 2018 rispetto allo stesso periodo dell’anno precedente. Infatti, nel febbraio 2018 un grande service provider nordamericano ha subito il maggiore attacco mai registrato, con un volume di ben 1,7 Tbps. Fortunatamente, la corretta progettazione e distribuzione dell’architettura del cliente, la sua capacità di risposta agli incidenti e la soluzione Arbor multistrato adottata contro gli attacchi DDoS hanno permesso di mitigare al meglio l’attacco, senza alcuna interruzione dell’attività. Ciononostante, questo attacco non fa che confermare una nuova realtà: le difese concepite per contrastare gli attacchi compresi nella fascia dei 300 Gbps sono ormai inadeguate e anche un’infrastruttura con capacità difensiva di 1 terabit non è esente da rischi.

L’ascesa degli attacchi da server Memcached

L’attacco di dimensioni record di febbraio è un esempio degli attacchi da server Memcached emersi nel corso del 2017, che sfruttano le vulnerabilità dei server di memoria cache utilizzati per accelerare l’accesso ai dati dei siti web. Memcached è un software open source gratuito frequentemente utilizzato nelle infrastrutture dei servizi cache e nelle reti aziendali allo scopo di incrementare la larghezza di banda. Gli autori dell’attacco di febbraio hanno scoperto una falla

nel design del pacchetto software Memcached, grazie alla quale sono riusciti a sfruttare grandi quantità di larghezza di banda del service provider per creare e lanciare un attacco di dimensioni mai viste prima.

Considerata la proliferazione dei software open source, spesso introdotti affrettatamente sul mercato e resi disponibili senza adeguati controlli sulle potenziali vulnerabilità, si può ragionevolmente ipotizzare che questo attacco sarà presto seguito da altri. I team di sicurezza dovrebbero pertanto prepararsi ad affrontare altri attacchi di impianto analogo. Del resto, man mano che gli strumenti vengono affinati ed emergono nuovi vettori di attacco, per i criminali informatici è sempre più facile ed economico lanciare attacchi più estesi ed efficaci.

La soluzione ibrida

Il trend dei grandi attacchi enfatizza la necessità di adottare una soluzione di difesa ibrida o stratificata, che riunisca funzioni di mitigazione on-premise e cloud. Gli attacchi più comuni hanno ancora dimensioni relativamente ridotte e possono essere generalmente individuati e mitigati con una soluzione on-premise (virtuale o fisica). Tuttavia, ora che le capacità degli aggressori hanno superato la soglia del terabit, è essenziale disporre di un componente basato su cloud capace di mitigare anche attacchi su larghissima scala. Il vantaggio dell'approccio ibrido consiste nella possibilità di utilizzare le difese basate su cloud come una sorta di riserva (diversamente dalle soluzioni "always on"), da attivare istantaneamente nel momento in cui il componente on-premise rilevi un attacco di grandi dimensioni.

Le soluzioni hardware e software contro gli attacchi DDoS risultano ancora più efficaci se sono supportate dalle informazioni sulle minacce globali. Con l'ausilio di questi dati e dell'analisi condotta da un valido team di ricerca, le misure contro le minacce note ed emergenti possono essere integrate direttamente nei prodotti di mitigazione.

Una lezione importante che abbiamo appreso dalla nostra pluriennale attività di analisi del panorama delle minacce informatiche è il fatto che, una volta entrati in scena, i nuovi tipi di attacchi DDoS non scompaiono spontaneamente. Il genio del terabit è uscito dalla lampada e non intende rientrarvi: dobbiamo prepararci ad affrontarlo.

A cura di: **Ivan Straniero**, Regional Manager Central & Southern Europe di NETSCOUT Arbor