Checklist per combattere gli attacchi DDoS a scopo di estorsione

Siete pronti a contrastare gli attacchi DDoS (Distributed Denial of Service) che continuano ad aumentare? Le organizzazioni che non hanno adottato una strategia di mitigazione degli attacchi DDoS potranno scegliere tra due alternative: pagare il riscatto o rischiare di incorrere in problemi di downtime imprevisti. Seguite questi passaggi per ridurre al minimo il rischio di attacchi DDoS a scopo di estorsione contro la vostra organizzazione.

1. Non date da mangiare agli orsi (immaginari e non)

Akamai consiglia di non effettuare pagamenti per riscatti o estorsioni: non esiste alcuna garanzia che l'autore dell'attacco darà seguito alle minacce o che il pagamento impedirà di sferrare l'attacco DDoS annunciato. Gli autori degli attacchi stanno tentando di sfruttare appieno la "paura dell'ignoto" per monetizzare rapidamente prima di passare all'obiettivo successivo.

2. Rivolgetevi ad esperti di mitigazione degli attacchi

Stabilite se le risorse aziendali più importanti e l'infrastruttura di back-end sono protette. Se non avete implementato controlli di mitigazione degli attacchi DDoS, rivolgetevi a fornitori di servizi sul cloud in grado di assistervi rapidamente in caso di emergenza (potete contattare la linea diretta di Akamai per la protezione dagli attacchi DDoS) per ridurre i rischi. I nostri specialisti dei SOCC globali combattono con successo contro gli attacchi DDoS da più di 20 anni.

3. Proteggetevi al meglio dagli attacchi DDoS

Con il giusto partner di mitigazione e i controlli di sicurezza appropriati, gli autori degli attacchi non hanno alcuna possibilità di successo. Per Akamai, quasi tutti gli attacchi DDoS associati a questa campagna sono stati mitigati in modo proattivo con il nostro SLA (accordo sul livello di servizio) immediato; solo una piccola percentuale ha richiesto una mitigazione attiva da parte del nostro SOCC globale. Anzi, circa il 70% di tutti gli attacchi mitigati nel 2020 è stato completamente bloccato grazie allo SLA (accordo sul livello di servizio) immediato di Prolexic.

4. Cambiate la vostra strategia di sicurezza

Basta un solo attacco per capire che i sistemi di difesa dagli attacchi DDoS sono fondamentali nell'attuale panorama delle minacce. Valutate la vostra capacità di reagire ai rischi per capire se un approccio alla mitigazione basato sul cloud on-demand o always-on sia più adatto per mantenere protetta la vostra presenza in Internet.

5. Riesaminate il vostro playbook per gli attacchi DDoS

Se non l'avete già fatto, riunite il personale IT e operativo, nonché i team dedicati alla sicurezza e alle comunicazioni con i clienti, per accertarvi di essere pronti e sapere cosa fare in caso di un attacco. Noi di Akamai abbiamo creato dei runbook di difesa personalizzati per ogni cliente, mettendo in atto varie strategie di risposta agli attacchi più comuni per assicurarci l'impiego delle persone, dei processi e delle procedure più appropriati al fine di ottimizzare la risposta agli incidenti.

Per garantire l'operatività delle risorse aziendali più importanti di oggi, le piccole e grandi imprese devono poter accedere a controlli di mitigazione di alta qualità, a una piattaforma scalabile e a competenze tali da arrestare le campagne di attacchi DDoS mirati. Visitate la pagina akamai.com/ddos-briefing per richiedere il vostro briefing sulle minacce DDoS personalizzato e ottenere informazioni utili per proteggere la vostra azienda.