[stato di internet] - security

ESAME DELL'ANNO

ANALISI RIASSUNTIVA: VOLUME 4, NUMERO 5

NOTE DEL REDATTORE

Da novembre 2017, il team di ricerca di Akamai ha pubblicato in media più di un articolo, post di blog e documento alla settimana, spaziando dai post sugli eventi imminenti, alle comunicazioni sulle minacce emergenti al rapporto sullo stato di Internet - Security. Ecco perché abbiamo deciso di rivedere il nostro lavoro sulla base del più ampio contesto della sicurezza a cui abbiamo assistito lo scorso anno. Consapevoli di ciò, abbiamo chiesto al nostro Chief Security Officer, Andy Ellis, di riflettere sulla direzione in cui potrebbero portarci nel 2019 le tendenze correnti. Di seguito un estratto del suo saggio.

UFFICIO DEL CSO

> **“ plus ça change, plus c’est la même chose -**
> Jean-Baptiste Alphonse Karr

Se c'è una verità nel settore della sicurezza in Internet, è che ogni anno è caratterizzato dall’incremento delle stesse tendenze. Nel 1998, durante l'operazione Desert Fox, gli avversari usarono un attacco DoS distribuito, che sfruttava anche la vulnerabilità *teardrop*, per provare a danneggiare le reti USCENTAF (all'epoca io ero tecnico addetto alla difesa, perciò mi ricordo l'entusiasmo nell'identificare l'attacco, eseguire i test di una configurazione e distribuirla al di fuori dei sistemi di sicurezza perimetrali). Tutto ciò non è strategicamente diverso da quanto si verifica nei centri operativi per la sicurezza (SOC), siano essi di proprietà di Akamai o no: sono solo cambiate le dimensioni e l'automazione.

Perciò, se guardiamo al 2019, è molto facile notare i modelli derivati dagli anni passati, suggerire che continueranno e supporre che probabilmente continueranno ad evolversi quasi nello stesso modo in cui hanno fatto finora.

Akamai
Experience the Edge

ATTACCHI DDOS DI FORZA BRUTA

Il DDoS è sempre un buon punto da cui iniziare, in gran parte perché le tendenze relative ai DDoS sono estremamente stabili. Potrebbe essere molto semplice pensare agli attacchi lungo due assi diversi: sfruttamento e larghezza di banda. La *larghezza di banda* è semplicemente la misurazione del traffico che un avversario può generare in un determinato momento. Storicamente, abbiamo visto crescere le dimensioni degli attacchi più grandi di circa il 9% a trimestre, vale a dire che sono raddoppiate ogni due anni. Tuttavia, è interessante notare che non si tratta di una crescita costante. Un nuovo picco viene raggiunto, insieme alla curva QoQ del 9%, ogni volta che un avversario scopre un nuovo modo per creare una botnet o una riflessione, come nel caso degli attacchi Mirai o degli attacchi di riflessione memcached.

Tra nuovi picchi, accadono due cose. Innanzitutto, le parti interessate, come amministratori di sistemi e operatori ISP, intraprendono le azioni necessarie per ridurre il numero di sistemi da poter usare per un attacco. In secondo luogo, gli avversari iniziano a lottare per il controllo di quelle risorse, pertanto le botnet iniziano a frammentarsi, riducendo le dimensioni dei singoli attacchi.

Dal punto di vista dell'efficacia, ciò non è in effetti deleterio per l'autore dell'attacco. In genere, le dimensioni degli stili di difesa DDoS non scalano in modo lineare. Gli attacchi più grandi avvengono ai margini della rete, nei punti in cui sono attivi servizi come Kona Site Defender o Prolexic Routed di Akamai. Le difese di medio livello sono ubicate al centro degli ISP e forniscono ai proprietari dei siti servizi di comunicazione "puliti". Le difese più piccole, sulle soluzioni in loco, risiedono solo all'interno dei data center di destinazione. Per un avversario la cui botnet non è sufficientemente grande per colpire un sistema di difesa situato ai margini della rete, un attacco a qualcuno che usa solo difese basate sui data center è comunque efficace, nonostante le dimensioni siano ridotte.

Dal momento che gli attacchi DDoS basati sulla larghezza di banda arrivano sotto diverse forme, è interessante notare che le dimensioni massime degli attacchi sembrano essere ristrette a una curva di crescita trimestrale del 9%. Interessante, ma non inspiegabile. Piuttosto che essere provocati da un qualche limite naturale, la spiegazione più probabile è che la crescita sottostante di Internet possa limitare la capacità di aggregazione delle botnet. La capacità di Internet attenua il danno totale che può generare un attacco DDoS: quanto più lontano si trova un obiettivo dai componenti di una rete, minore sarà il traffico che confluirà nei collegamenti congestionati tra l'obiettivo e la sorgente dell'attacco.

Per conoscere meglio il punto di vista di Andy sugli attacchi DDoS, a livello di applicazione, di credential stuffing, gig economy e blockchain, potete scaricare il rapporto **Stato di Internet - Security: esame dell'anno**, Volume 4, Numero 5.

INFORMAZIONI SU AKAMAI

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. La piattaforma edge intelligente di Akamai permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per la edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24/7/365. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito https://www.akamai.com/it/it/ o https://blogs.akamai.com/it/ e seguite @AkamaiItalia su Twitter. Le nostre informazioni di contatto globali sono disponibili su https://www.akamai.com/it/it/locations oppure chiamando il numero +39 02 006214. Data di pubblicazione: 12/18.