SOTI - ESTATE 2018

[stato di internet]/sicurezza

ANALISI RIASSUNTIVA

Analisi riassuntiva

Akamai, la piattaforma di cloud delivery più ampia e affidabile a livello mondiale, utilizza la sua Akamai Intelligent Platform™ distribuita su scala globale per elaborare migliaia di miliardi di transazioni Internet ogni giorno. In questo modo raccoglie enormi quantità di dati correlati alla connettività a banda larga, alla sicurezza sul cloud e alla distribuzione di contenuti media. Ogni trimestre, Akamai pubblica *i rapporti sullo stato di Internet* basati su questi dati, focalizzandosi sulla connettività a banda larga e sulla sicurezza sul cloud.

IMPLICAZIONI AZIENDALI

Gli attacchi a cui abbiamo assistito negli ultimi mesi ci ricordano che lo stato della sicurezza in Internet non è mai statico. L'ingegno degli autori degli attacchi non si ferma mai: vengono continuamente scoperti nuovi vettori e sfruttate nuove vulnerabilità, nell'intento di sviluppare strategie di attacco che risultano più dannose che mai. Nel 2017, abbiamo assistito alla nascita dello sfruttamento di nuove classi di dispositivi, come i telefoni cellulari e i dispositivi IoT, di cui botnet di grandi dimensioni si sono avvalse per sferrare attacchi record. Ma già nei primi due mesi del 2018, i record precedenti sono stati superati, poiché gli autori degli attacchi hanno scoperto un nuovo vettore, il servizio memcached - originariamente non destinato ad essere esposto su Internet - per generare attacchi che superano la paralizzante cifra di 1 Tbps. Il servizio memcached consente di amplificare gli attacchi per ordini di grandezza sempre maggiori rispetto a qualsiasi attacco di riflessione precedentemente noto.

Fortunatamente, in questo caso, una risposta tempestiva da parte di sviluppatori, operatori di rete e provider di servizi sembra aver ridotto rapidamente il numero dei server memcached vulnerabili disponibili, limitando il potenziale di questo nuovo vettore di attacco per il futuro. Ciò ricorda alquanto prepotentemente che la comunità per la sicurezza non può mai riposare sugli allori, ma che dobbiamo essere consapevoli delle tendenze degli attacchi e dei progressi della tecnologia, per prepararci al crescere della loro portata. Inoltre, è impegno di tutta la comunità tenersi aggiornati con le patch software e le configurazioni di sicurezza al fine di ridurre al minimo l'accesso alle superfici soggette ad attacchi da parte dei criminali.

PANORAMICA DEL REDATTORE

Il presente rapporto continua ad evolversi così come lo stato della sicurezza su Internet. Stiamo attuando i necessari cambiamenti alla frequenza, al formato e alla struttura della pubblicazione, nell'intento di fornirvi informazioni dettagliate provenienti da tutti i nostri dati e dalle ricerche da noi condotte nel modo più tempestivo e rilevante possibile. Gran parte dei dati statistici e dei grafici sugli attacchi DDoS e alle applicazioni web (compresi i grafici sulla frequenza del vettore e sulle dimensioni degli attacchi DDoS) è stata spostata sul nostro sito web. Potete trovare eventuali aggiornamenti nel nostro blog. Inoltre, pubblicheremo regolarmente rapporti più brevi e semplificati per concentrarci su tendenze, ricerche e analisi relative ad un periodo più lungo. Il rapporto *Stato di Internet/Sicurezza: gli attacchi web* verrà ora pubblicato due volte all'anno in estate e in inverno.

La nostra analisi degli attacchi dell'estate 2018 si concentra sull'attacco di riflessione memcached di febbraio 2018, che ha stabilito un nuovo record come il più grande attacco mai mitigato da Akamai fino ad ora. Con i suoi 1,3 Tbps, l'attacco ha più che raddoppiato il record precedente di 623 Gbps raggiunto da Mirai nel settembre

1 Tbps

Soglia infranta dall'attacco di riflessione memcached

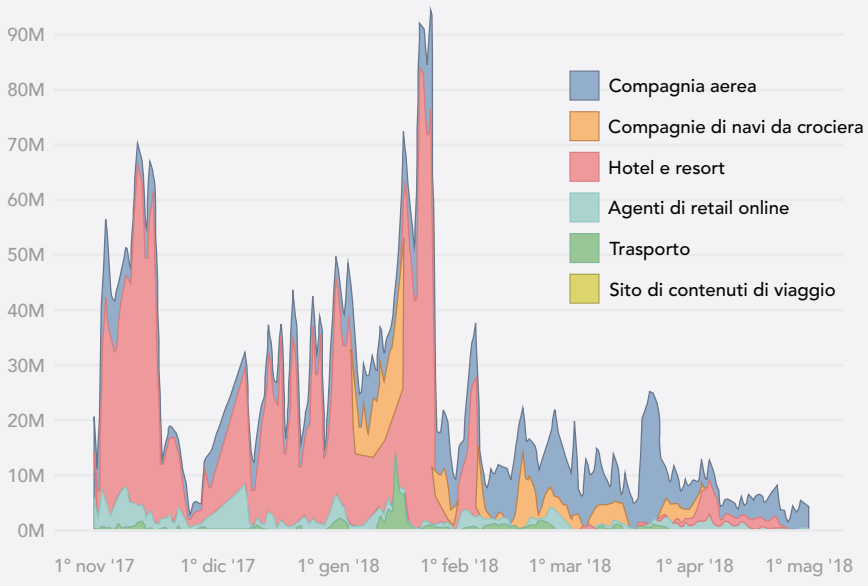
2016. Le dimensioni medie degli attacchi DDoS hanno continuato ad aumentare negli ultimi anni, raggiungendo ora una cifra di 1,3 Gbps, il che sottolinea l'importanza per ogni organizzazione di prepararsi all'eventualità di subire attacchi su larga scala.

Nel rapporto *Stato di Internet/Sicurezza: gli attacchi web dell'estate 2018*, esamineremo alcuni attacchi DDoS che impiegano tattiche inconsuete per aumentare la loro efficacia. Mentre la maggior parte degli attacchi DDoS sono intrinsecamente semplici e volumetrici, pochi di essi mostrano l'influenza di nemici intelligenti e adattivi che cambiano tattica per superare le difese a modo loro.

Operation Power Off, un'iniziativa delle forze dell'ordine per chiudere i siti DDoS-for-hire, è un argomento di grande interesse. Uno sforzo coordinato nell'aprile 2018 tra varie forze dell'ordine in più paesi ha consentito di far chiudere il sito Webstresser.org, che ha svolto un ruolo importante nel mercato dei siti DDoS-for-hire, rendendosi, presumibilmente, responsabile di milioni di attacchi. Considerando quanto siano redditizi questi siti, non deve sorprendere se verranno soppiantati a breve da altri siti dello stesso tipo.

Infine, basandoci sui dati relativi all'abuso di credenziali e bot che abbiamo analizzato in primo luogo nel rapporto *Stato di Internet/Sicurezza* del quarto trimestre 2017, abbiamo condotto un'analisi più approfondita per caratterizzare e comprendere meglio gli autori degli abusi di credenziali e bot che mirano al settore alberghiero, il mercato verticale che ha registrato la più alta percentuale di accessi dannosi fino ad ora. Abbiamo anche notato che la chiusura di vari percorsi all'inizio di febbraio 2018 sembra aver fatto calare in picchiata il traffico dannoso.

Figura 1.1 **Tentativi di accesso dannosi: hotel e viaggi**



ATTACCHI DDOS

CONFRONTO TRA L'ESTATE 2018 E L'ESTATE 2017

16% di aumento degli attacchi DDoS totali

16% di aumento degli attacchi a livello di infrastruttura (livelli 3 e 4)

4% di aumento degli attacchi basati su tecniche di riflessione

38% di aumento degli attacchi a livello di applicazioni

Per i dettagli dell'analisi e della ricerca, scaricate il rapporto integrale.

Il rapporto *Stato di Internet/Sicurezza: gli attacchi web dell'estate 2018* combina i dati sugli attacchi raccolti in tutta l'infrastruttura globale di Akamai e rappresenta le ricerche svolte da vari team diversificati in tutta l'azienda.

STATO DI INTERNET/TEAM ADDETTO ALLA SICUREZZA

Jose Arteaga, Akamai SIRT, Data Wrangler - Analisi degli attacchi
Dave Lewis, Global Security Advocate - Operation Power Off
Wilber Mejia, Akamai SIRT - Analisi degli attacchi
Elad Shuster, Security Data Analyst Advanced DDoS - Blog di Akamai
David McEwan, Security Operations Command Center - Advanced DDoS
Alejandro Ziegenhirt, Security Operations Command Center - Advanced DDoS

RESPONSABILI EDITORIALI

Martin McKeay, Senior Security Advocate, Senior Editor
Amanda Fakhreddine, Senior Technical Writer, Editor

TEAM CREATIVO

Shawn Broderick e Sajeesh Alakkaparambil, Design
Georgina Morales Hampe e Kylee McRae, Project Management

INFORMAZIONI SU AKAMAI

Grazie alla propria piattaforma di cloud delivery più estesa e affidabile al mondo, Akamai supporta i clienti nell'offerta di experience digitali migliori e più sicure da qualsiasi dispositivo, luogo e momento. Con oltre 200.000 server in 130 paesi, la piattaforma Akamai garantisce protezione dalle minacce informatiche e performance di altissimo livello. Il portfolio Akamai di soluzioni per le web e mobile performance, la sicurezza sul cloud, l'accesso remoto alle applicazioni aziendali e la delivery di contenuti video è affiancato da un servizio clienti affidabile e da un monitoraggio 24x7. Per scoprire perché i principali istituti finanziari, i maggiori operatori e-commerce, provider del settore Media & Entertainment ed enti governativi si affidano ad Akamai, visitate il sito https://www.akamai.com/it/it/ e https://blogs.akamai.com/it/ o seguite @AkamaiItalia su Twitter. Le nostre informazioni di contatto globali sono disponibili su www.akamai.com/locations oppure chiamando il numero +39 02 006214. Data di pubblicazione: 06/18.