[stato di internet] / security

Analisi riassuntiva Q3 2017

Akamai

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 media delivery. *Stato di Internet* è stato creato per sfruttare tali dati e supportare aziende e governi nell'adozione di decisioni strategiche migliori. Ogni trimestre Akamai utilizza questi dati per pubblicare i rapporti sullo Stato di Internet, focalizzati sulla connettività a banda larga e sulla sicurezza sul cloud.

Il *Rapporto sullo stato di Internet / Security* Q3 2017 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.

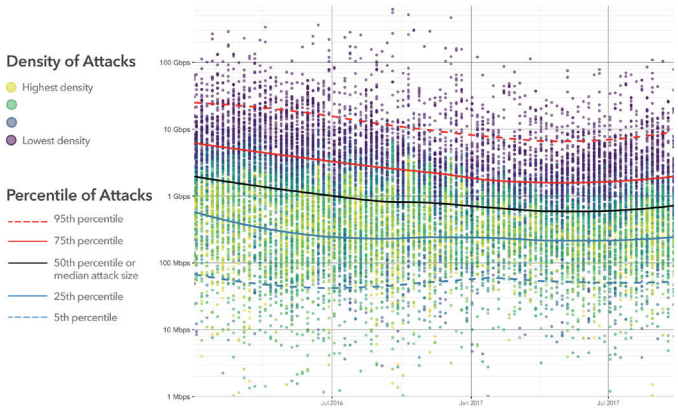
Implicazioni per le aziende / I titoli dei media del terzo trimestre hanno messo in evidenza la pesante ricaduta in termini finanziari e commerciali causata dagli attacchi informatici sulle aziende di numerosi settori. I nostri dati dimostrano che gli attacchi sono in aumento all'approssimarsi della stagione critica delle festività di fine anno, con una chiara implicazione: ignorare la cyber sicurezza comporta rischi altissimi. Questo è esattamente ciò di cui Chris Wysopal, co-fondatore e CTO di Veracode e invitato speciale per questo trimestre, ha iniziato ad avvertire il mondo quasi due decenni fa.

Come requisito minimo, le organizzazioni devono mantenere software e firmware aggiornati e al corrente con le patch, mentre la protezione dagli attacchi DDoS deve costituire parte integrante dei piani e dei preparativi per i livelli di traffico delle festività. Una rivalutazione costante dei rischi a cui sono esposte le aziende non è un optional: è assolutamente essenziale. Capire le strategie in evoluzione degli aggressori è indispensabile per opporre difese più efficaci ai loro attacchi. Il rapporto SOTI/S di questo trimestre esamina nei dettagli l'ascesa e il declino di WireX, la nuova botnet basata su Android, e presenta i risultati di una ricerca sulle reti Fast Flux utilizzate dalle botnet per nascondere le proprie attività dannose e mimetizzare le proprie comunicazioni CnC (Command and Control), rendendone molto più difficile il rilevamento.

Sintesi editoriale / Di recente i media hanno dato spazio ad alcuni tra i più estesi incidenti di cyber sicurezza mai visti finora, dalla rivelazione di Yahoo sulla manomissione di tutti i suoi 3 miliardi di account alla violazione di Equifax che ha messo a in pericolo i dati sensibili di 146 milioni di americani. Nel frattempo sono arrivate le prime stime del grave impatto finanziario dell'attacco ransomware NotPetya del secondo trimestre, che è costato a più di un'azienda centinaia di migliaia di dollari.

Se questi sono gli incidenti che meritano titoli sui giornali, la realtà è che gli attacchi più comuni, come gli attacchi DDoS e alle applicazioni web, possono essere altrettanto dannosi per un'organizzazione. Questi attacchi si verificano con frequenza sempre maggiore contro aziende di ogni dimensione e in tutti i settori. Nel TERZO TRIMESTRE, Akamai ha registrato un aumento su base trimestrale sia del numero degli attacchi DDoS sia di quello degli attacchi alle applicazioni web, rispettivamente dell'8% e del 30%. Anche le dimensioni medie degli attacchi sono aumentate, come pure la frequenza degli attacchi per cliente colpito.

Densità degli attacchi e tendenze, gennaio 2017 – settembre 2017



Benché le piattaforme e i vettori di attacco tradizionali siano sempre diffusi ed efficaci, i criminali informatici continuano a sviluppare il proprio arsenale. Nel corso di questo trimestre hanno continuato a sfruttare il malware Mirai, che utilizza dispositivi IoT, e allo stesso tempo hanno introdotto WireX, che prende il controllo dei dispositivi Android. Entrambi i vettori evidenziano le vaste riserve potenziali di nuove reclute per gli eserciti delle botnet.

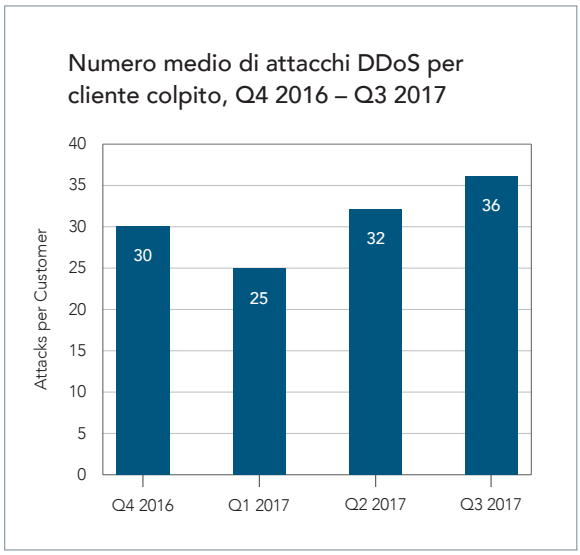
Aggiornamento DDoS / Gli attacchi DDoS (Distributed Denial of Service) sono costosi: possono paralizzare i siti, interrompere le attività aziendali e distrarre risorse. Possono anche essere utilizzati come copertura per violazioni più insidiose dei dati o dei sistemi. Nel terzo trimestre, gli attacchi DDoS hanno proseguito il trend in crescita del SECONDO TRIMESTRE, aumentando ancora dell'8%. Anche il numero medio di attacchi DDoS per cliente colpito ha continuato a crescere, raggiungendo quota 36, ossia una media di più di uno ogni tre giorni. Nel caso più estremo, un singolo cliente del settore gaming ha subito 612 attacchi DDoS nel solo terzo trimestre: una media di quasi sette attacchi al giorno per tutto il trimestre.

ATTACCHI DDoS [Q3 2017 rispetto a Q2 2017]

- Aumento dell'8% degli attacchi DDoS totali
- Aumento dell'8% degli attacchi a livello di infrastruttura (livelli 3 e 4)
- Aumento del 4% degli attacchi basati su tecniche di riflessione
- Aumento del 13% del numero medio di attacchi per cliente colpito

Gli attacchi DDoS del terzo trimestre hanno utilizzato molti vettori di attacco già noti. La famiglia di malware Mirai ha sfruttato innumerevoli dispositivi IoT (Internet of Things) per generare alcuni dei più massicci attacchi DDoS mai registrati: il più grande rilevato da Akamai ha raggiunto i 623 Gbps. Benché oggi Mirai non sia più così attiva, questa botnet continua a rappresentare una minaccia e nel terzo trimestre è stata di nuovo responsabile del più grande attacco registrato, con un picco di 109 Gbps.

Nel terzo trimestre è anche comparsa per la prima volta WireX, degna di nota non solo per essere stata una delle prime botnet di grandi dimensioni basate su Android, ma anche per il modo in cui si è propagata. I consumatori in tutto il mondo scaricavano inconsapevolmente il malware attraverso app infette apparentemente legittime in Google Play Store. Benché WireX si sia diffusa rapidamente, uno sforzo congiunto di varie aziende, tra cui Akamai, ha dimostrato la potenza della collaborazione tra settori riuscendo ad arrestare WireX prima che raggiungesse dimensioni rilevanti. Si prevede tuttavia che WireX, come Mirai, continuerà ad essere presente, a evolversi e a proliferare. Le organizzazioni devono prepararsi all'eventualità che si verifichino in qualsiasi momento attacchi DDoS di dimensioni molto maggiori, dato che vengono continuamente sviluppate nuove tecniche.



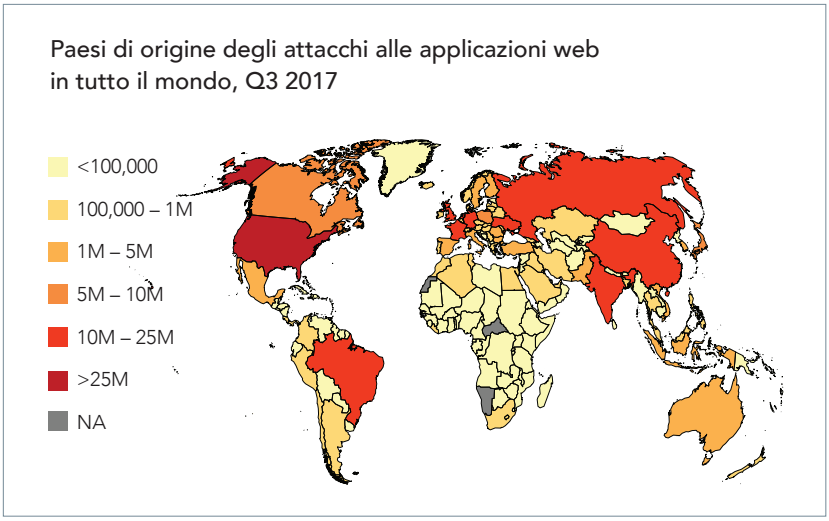
Aggiornamento sugli attacchi alle applicazioni web / A differenza degli attacchi DDoS, che cercano di sovraccaricare il sito web, gli attacchi alle applicazioni web tendono a prendere di mira le vulnerabilità delle applicazioni per rubare dati o compromettere in altro modo il sistema sottostante. Gli attacchi alle applicazioni web sono molto più comuni degli attacchi DDoS e la loro frequenza li rende più facili da ignorare, e quindi potenzialmente più dannosi. Purtroppo gli attacchi di questo tipo continuano a infittirsi da un trimestre all'altro, con un salto del 30% nella frequenza degli attacchi nel terzo trimestre. L'85% degli attacchi ha sfruttato SQL injection o LFI (Local File Inclusion), i due principali vettori di attacco.

ATTACCHI ALLE APPLICAZIONI WEB [Q3 2017 rispetto a Q2 2017]

- Aumento del 30% degli attacchi alle applicazioni web totali
- Aumento del 48% degli attacchi con origine negli Stati Uniti (principale paese di origine)
- Aumento del 19% degli attacchi SQLi

Gli Stati Uniti continuano a essere nettamente in testa sia come origine che come destinazione della maggior parte del traffico relativo agli attacchi alle applicazioni web registrato da Akamai. Nel terzo trimestre, gli Stati Uniti hanno fatto registrare più di 300 milioni di attacchi alle applicazioni web, circa cinque volte il numero riscontrato in Russia, il paese che li segue al secondo posto.

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



***Stato di Internet / Security*: il team**
Jose Arteaga, SIRT Lead Akamai, Data Wrangler — Analisi degli attacchi
Dave Lewis, Global Security Advocate — Attività DDoS, attività degli attacchi alle applicazioni web
Chad Seaman, SIRT Akamai — Analisi degli attacchi, cluster Command and Control di Mirai
Wilber Mejia, SIRT Akamai — Analisi degli attacchi
Alexandre Laplume, SIRT Akamai — Analisi degli attacchi
Elad Shuster, Security Data Analyst, unità Threat Research
Or Katz, Principal Lead e Security Researcher — DGA (algoritmi di generazione dei domini)
Jon Thompson, Custom Analytics
Shrijita Bhattacharya, Intern — cluster Command and Control di Mirai

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

Design
Shawn Doughty, Creative Direction
Brendan O'Hara, Art Direction/Design

Contatti
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@akamaiItalia*
www.akamai.com/stateoftheinternet-security

Scaricate la versione integrale del rapporto

[stato di internet] / security
Rapporto integrale Q3 2017