Sviluppo di un piano strategico di prevenzione e di mitigazione degli incidenti di sicurezza per garantire la continuità operativa.

‘ La Cloud intelligence come deterrente alle nuove minacce di cybercrime e cyberwarfare '

Mr. Paolo Bufarini - Head of Security, Italy and Mediterranean Region, Akamai

Agenda

- INTRODUZIONE
  - IL PANORAMA DELLE MINACCE IN RAPIDO CAMBIAMENTO
  - I TRADIZIONALI APPROCCI DI SICUREZZA PER LA DIFESA DAI CYBER ATTACCHI
  - LA NECESSITA' DI UNA DIFESA PROATTIVA
  - LA AKAMAI INTELLIGENT PLATFORM
- CONCLUSIONI

INTRODUZIONE

- Oggi le aziende operano in un mondo veloce in rapida evoluzione. **Entro la fine del 2016, quasi 3,5 miliardi di persone saranno collegate ad Internet**, spesso attraverso molteplici dispositivi di elaborazione. La gente sta spendendo una quota crescente della loro vita on-line – per comunicazione, shopping, intrattenimento e per lavoro. Per organizzazioni imprenditoriali e governative, questo rappresenta un cambiamento significativo nel modo di interagire con i propri clienti e dipendenti.

- Per queste organizzazioni, la maggior parte delle loro attività quotidiane ora si svolgono al di fuori dell'ufficio tradizionale. Si interfacciano con i clienti e collaborano con i colleghi su Internet per l'esecuzione di transazioni finanziarie, la trasmissione di dati aziendali sensibili, comunicando su reti pubbliche.

- Per fare questo stanno portando gran parte delle loro applicazioni su reti con accesso ad Internet, così i clienti possono fare acquisti 24x7 e i dipendenti possono accedere alle risorse di cui hanno bisogno in qualsiasi momento nel corso della giornata di lavoro globale.

INTRODUZIONE (Cont'd)

- Come risultato gli attaccanti possono più facilmente accedere ad un numero maggiore valore di asset aziendali e governativi.
- Gli aggressori hanno spostato di conseguenza i loro metodi con lo sviluppo di nuovi attacchi
- Il panorama delle minacce è in continua e rapida evoluzione
- Quando si confrontano diversi approcci alla sicurezza, le organizzazioni devono prendere in considerazione i punti di forza e di debolezza di ogni soluzione - non solo come svolge la difesa contro gli attacchi di oggi, ma anche come ben risponderà a quelli di domani.
- Determinare l'efficacia di qualsiasi soluzione di sicurezza a lungo termine.

Ricorrenti minacce cyber

- Indipendentemente da come viene gestita la sicurezza informatica, la conoscenza del settore industriale o commerciale è fondamentale per la costruzione di una difesa contro i tipi più comuni di oggi di minacce informatiche, che comprendono:

1. Data breaches
2. Denial of Service (DoS) e Distributed Denial of Service (DDoS)
3. Hacktivism
4. Website defacement

Gli attacchi Denial-of-service sono in continua crescita

- Una delle minacce oggi più comuni e diffuse di sicurezza è l'attacco di negazione del servizio (DoS). Attacchi DoS tentano di interrompere un servizio internet critico o di una componente di infrastruttura.

- Il primo attacco DoS documentato pubblicamente ha avuto luogo il 6 settembre 1996 contro Panix, un ISP basato a New York City.

- Gli attaccanti moderni impiegano sia grandi botnet o tecniche di riflessione con un traffico attacco di diversi ordini di grandezza maggiore in termini di magnitudine.

- Entro il 2020 , Akamai prevede che l'attacco DDoS medio genererà 1,5 Tbps di traffico di rete.

- Questa rapida crescita evidenzia la difficoltà nella difesa contro gli attacchi DDoS volumetrici.

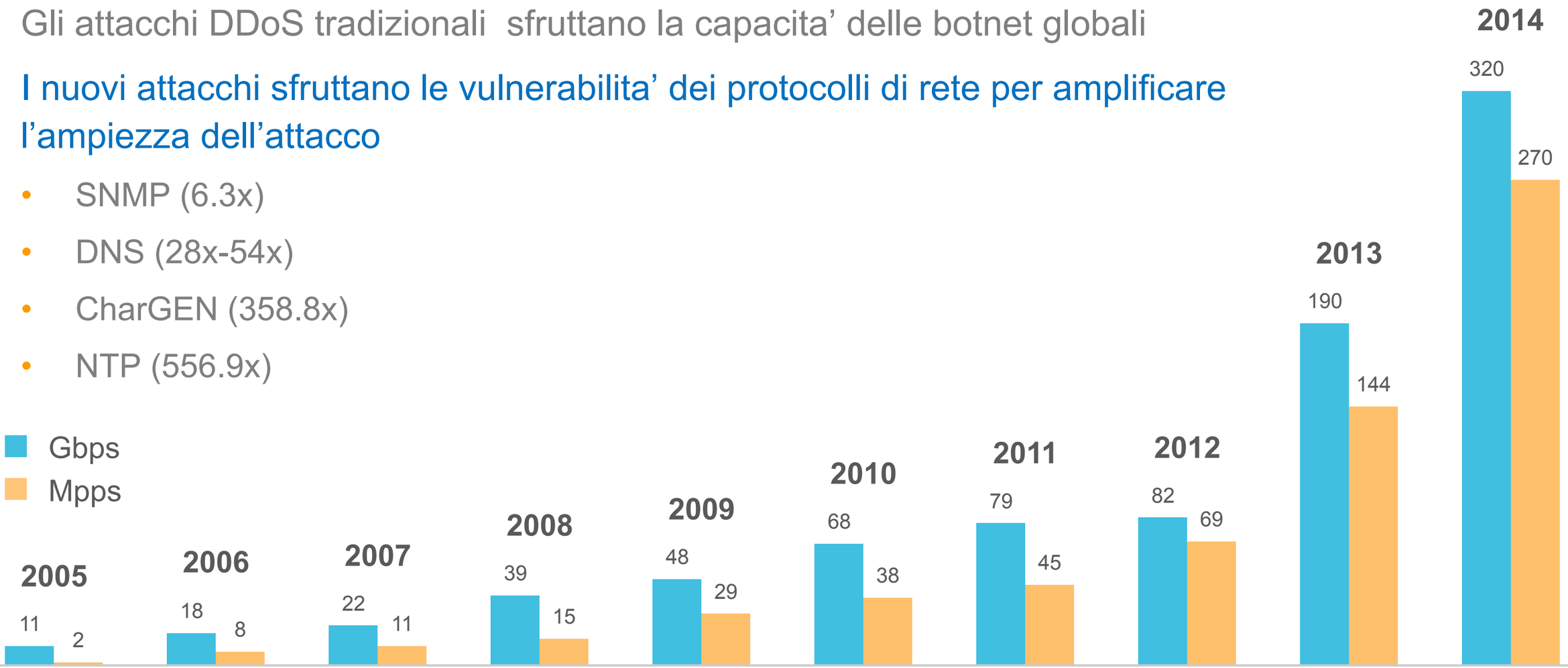
- Questi attacchi sfruttano la potenza di Internet per scalare al di là delle risorse finanziarie e tecnologiche delle singole organizzazioni.

Gli attacchi Denial-of-Service sono in continua crescita (Cont'd)

Gli attacchi DDoS tradizionali sfruttano la capacita' delle botnet globali

I nuovi attacchi sfruttano le vulnerabilita' dei protocolli di rete per amplificare l'ampiezza dell'attacco

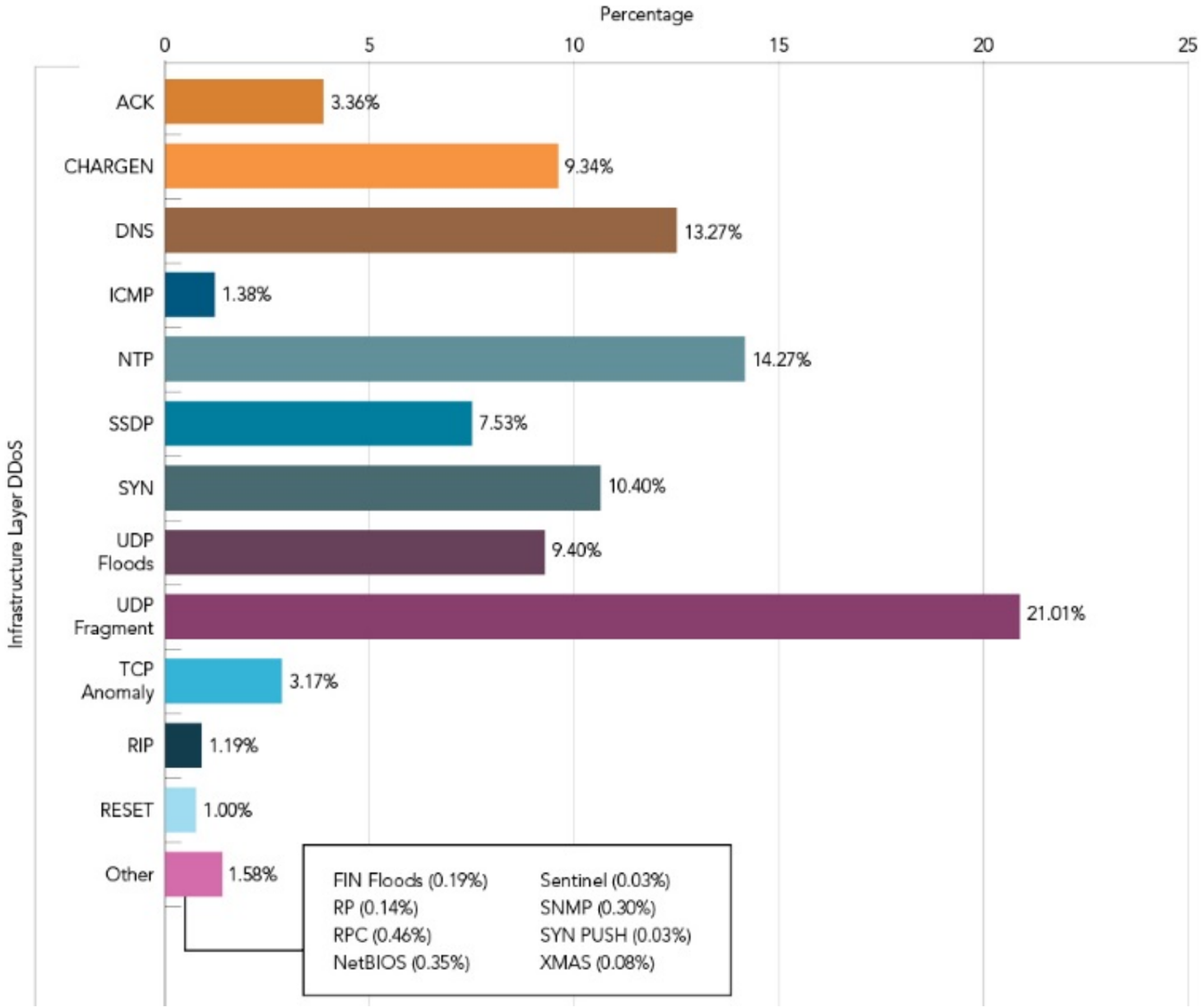
- SNMP (6.3x)
- DNS (28x-54x)
- CharGEN (358.8x)
- NTP (556.9x)

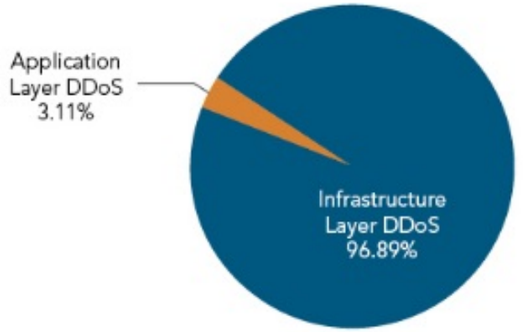


Gli attacchi si stanno spostando verso il livello di applicazione

- Mentre gli attacchi a livello di rete continueranno a rappresentare una sfida significativa a causa della loro scala, gli attacchi DDoS mirati a livello di applicazione potranno rivelarsi una sfida più complessa a lungo termine.
- I clienti Akamai hanno segnalato 1553 attacchi DDoS a livello applicativo nel 2015.
- Gli attacchi DDoS a livello applicativo sono più difficili da rilevare che gli attacchi a livello di rete perché assomigliano al traffico di rete legittimo.
- Ad esempio i Flood HTTP generano alti volumi di richieste HTTP legittime al server Web di destinazione, bypassando gli strumenti di sicurezza tradizionali incentrati sul livello di rete , mentre i server Web in genere non hanno la capacità di distinguere oggi tra il traffico normale e quello di attacco.

Tipologie di attacchi DDoS & Relativa distribuzione in Q4 2015



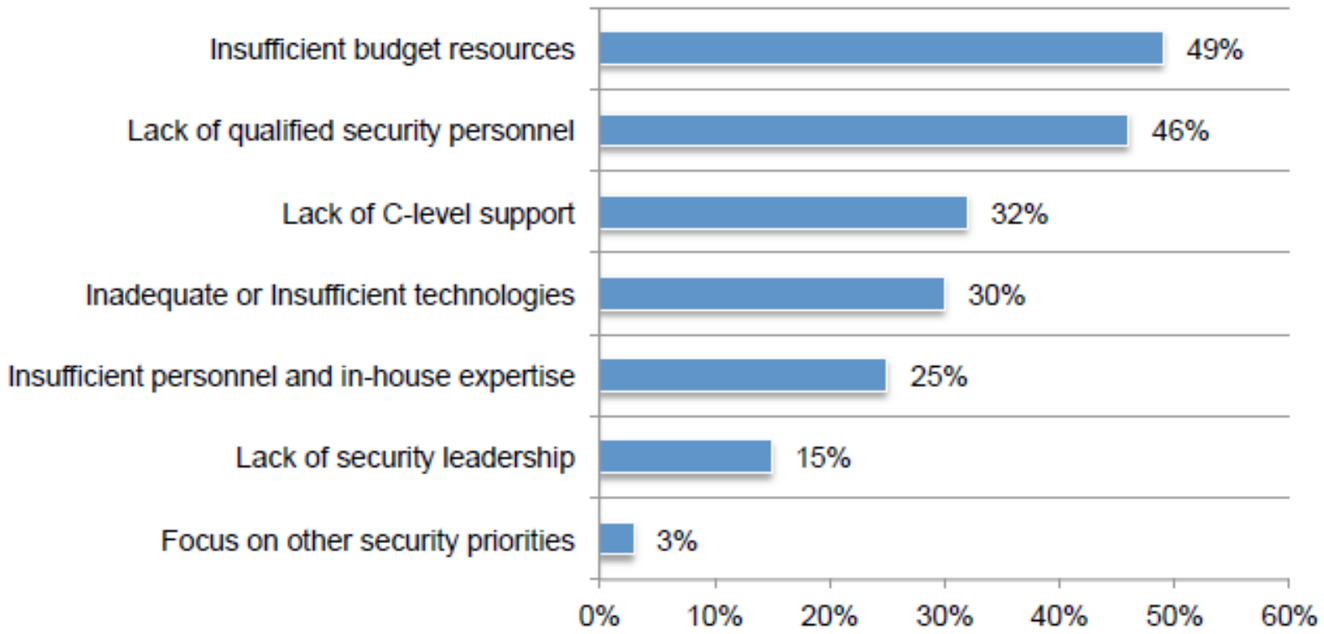


UDP Fragment, NTP, SYN and DNS attack vectors made up almost 60% of the attacks.

Gli attacchi si stanno spostando verso il livello di applicazione (Cont'd)

- Un ostacolo nel fermare gli attacchi DoS-DDoS è la mancanza di risorse aziendali. Le barriere più critiche per prevenire queste minacce sono risorse di bilancio insufficienti, mancanza di personale qualificato alla sicurezza (46 per cento) e la mancanza di supporto a livello dirigenziale, come mostrato nella figura seguente.

Figure 6. Barriers to preventing DoS attacks
Two responses permitted



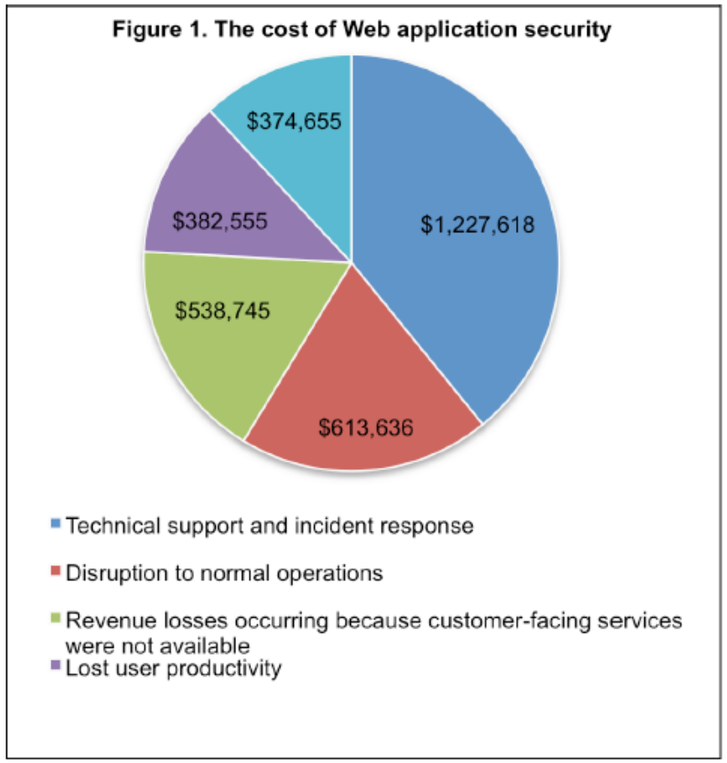
Ponemon INSTITUTE

Incremento della frequenza e dei costi del cybercrime

- Non solo il numero, la varietà e il valore in costi finanziari di obiettivi stanno proliferanno, ma le barriere per lo svolgimento di un attacco di successo sono cadute.
- La facile divulgazione dei toolkit per l'attaccante e la facilità con cui le vulnerabilità scoperte di recente possono essere condivise hanno notevolmente democratizzato il crimine informatico. Come risultato le aziende stanno sperimentando attacchi più frequentemente.
- Il Ponemon Institute ha recentemente riportato un aumento del 18 per cento nel numero di attacchi riusciti tra gli intervistati nel 2015.
- Questi attacchi stanno imponendo un maggior costo finanziario.
- Ma forse anche piu' rischioso, le imprese spesso memorizzano le informazioni sensibili in archivi centralizzati che possono essere accessibili attraverso un browser web. Questi database presentano obiettivi interessanti per gli attaccanti ricercare un guadagno economico.
- Una volta rare, le violazioni dei dati sono ora la tipologia più pubblicizzata di crimine informatico.

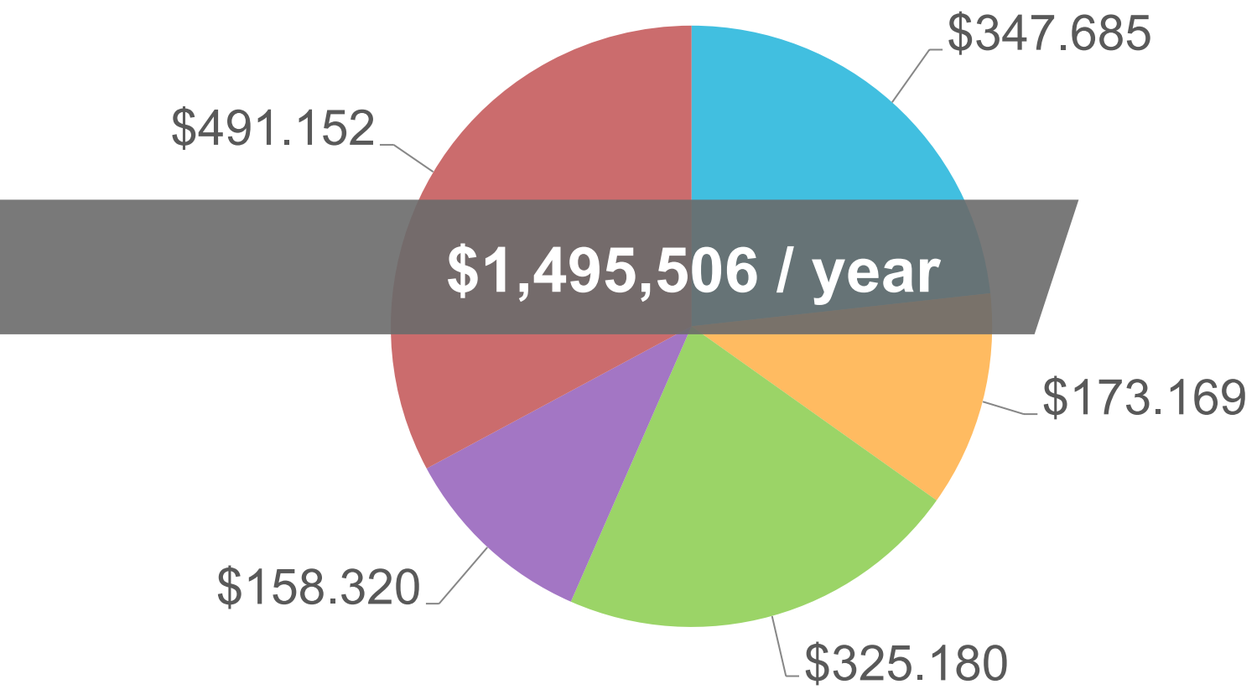
Incremento della frequenza e dei costi del cybercrime (Cont'd)

- La sicurezza delle applicazioni Web è considerata altrettanto critica o più critica di altri problemi di protezione affrontati dalle organizzazioni. Con gli incidenti di sicurezza delle applicazioni Web che stanno diventando sempre più comuni, gli intervistati ritengono che gli attacchi alle applicazioni Web sono costati loro organizzazioni circa 3,1 $ milioni negli ultimi 12 mesi. Come mostrato nella figura in basso, la maggior parte del costo è dovuto al supporto tecnico necessario e risposta agli incidenti .



Incremento della frequenza e dei costi del cybercrime (Cont'd)

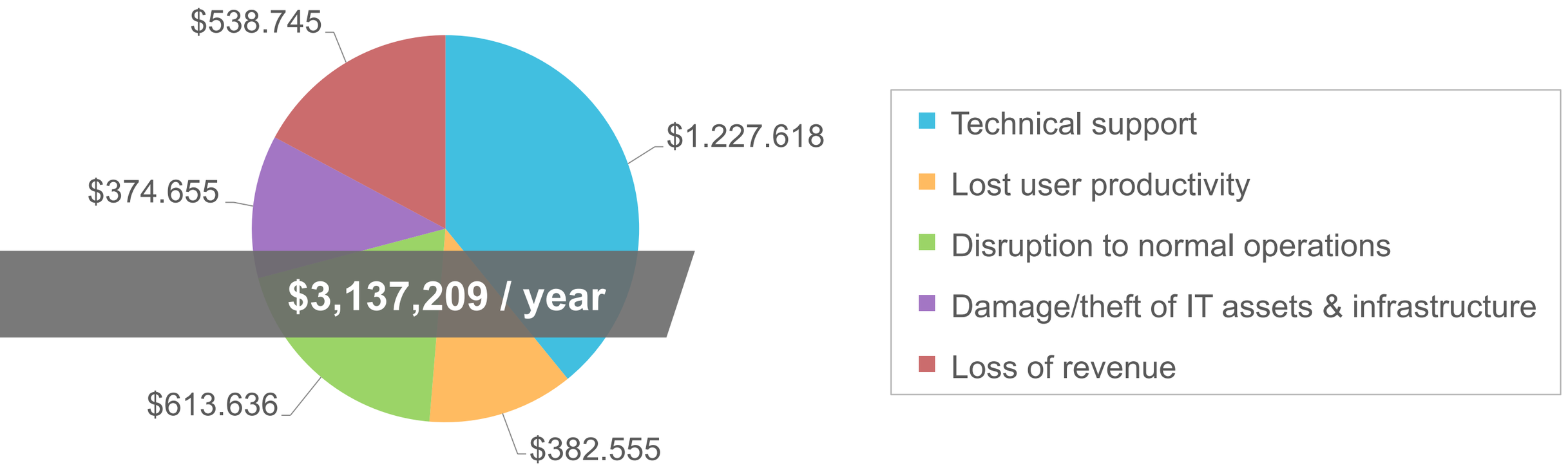
Total Cost of DoS Attacks



Source: The Cost of Denial-of-Service Attacks, Ponemon Institute

Incremento della frequenza e dei costi del cybercrime (Cont'd)

Total Cost of Web Application Attacks

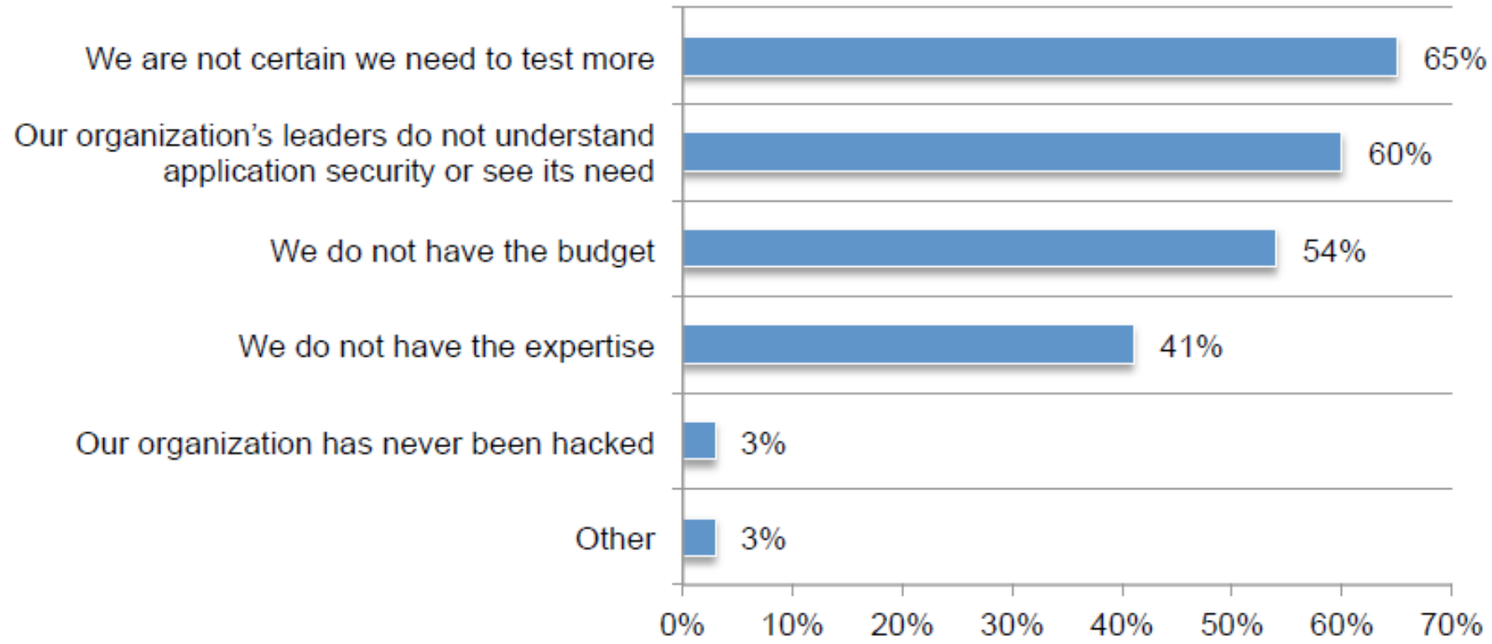


Source: Ponemon Institute, 2015

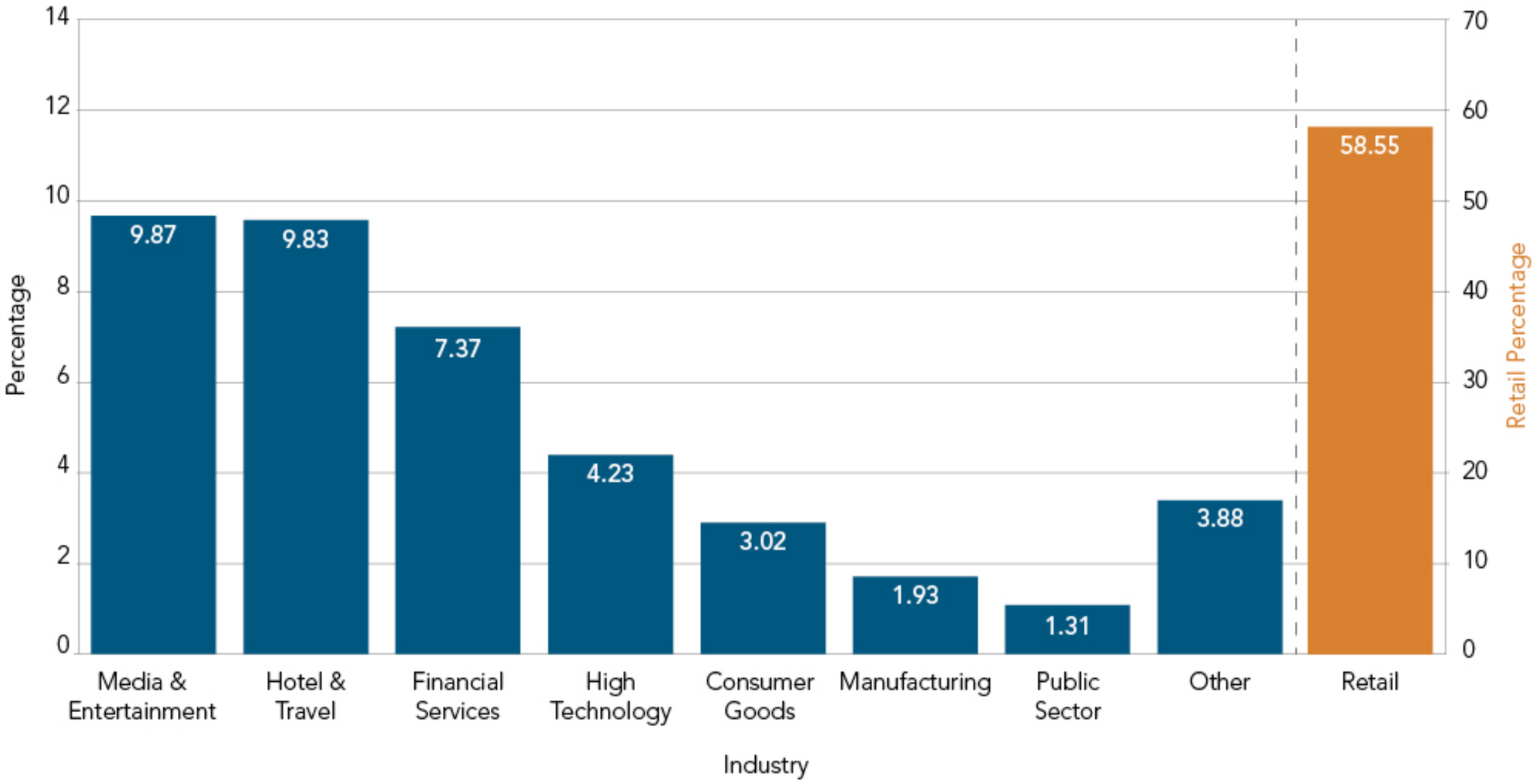
Incremento della frequenza e dei costi del cybercrime (Cont'd)

- Nonostante quanto frequentemente le applicazioni Web sono compromesse, in media meno della metà di esse sono testate. Le ragioni principali per non testare le applicazioni Web sono: incertezza su quanto testare, il senior management non capisce la sicurezza delle applicazioni o non ne comprende il bisogno, nessun bilancio e nessuna competenza in azienda sono disponibili.

Figure 12. Why organizations don't test Web applications
More than one response permitted



Attacchi alle applicazioni Web per settore di mercato, Q4 2015



As in previous quarters, the retail industry was most frequently targeted with web application attacks in Q4 2015

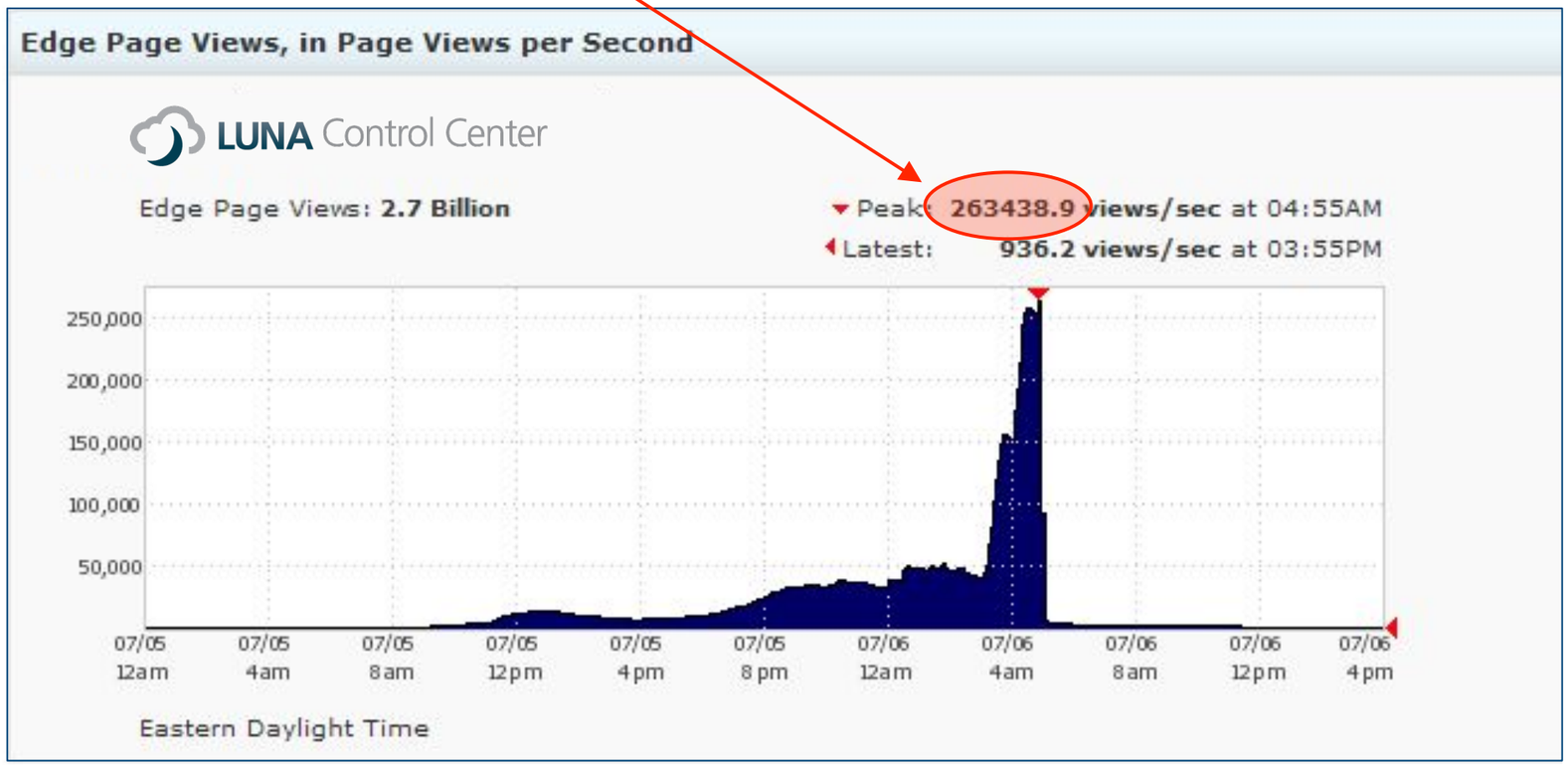
Una minaccia multi-dimensionale per la sicurezza

- Mentre molte soluzioni di sicurezza si concentrano sulla difesa contro un singolo tipo di attacco, gli aggressori stanno sempre più impiegando più tipi differenti di attacchi in combinazione.
- Attacchi Multi-dimensionali hanno una maggiore probabilità di successo
- Inoltre, gli aggressori stanno iniziando a combinare attacchi DDoS con attacchi SQL, usando gli attacchi di banda DDoS rumorosi per distrarre risorse di sicurezza limitate dal vero obiettivo dell'attaccante che e' quello del furto di dati o finanziario.
- Ci sono stati almeno tre esempi pubblici delle istituzioni finanziarie attaccati in questo modo a metà del 2013, in cui gli aggressori hanno rubato milioni di dollari durante la confusione.
- Questo scenario mette in evidenza il pericolo di concentrarsi su di un solo tipo di vettore di attacco.
- Le organizzazioni devono essere preparate a rispondere ad una serie di potenziali attacchi, tra cui le combinazioni di diversi tipi di attacchi, al fine di salvaguardare la propria infrastruttura IT.

Case Study – Stock Exchange DDoS Attack

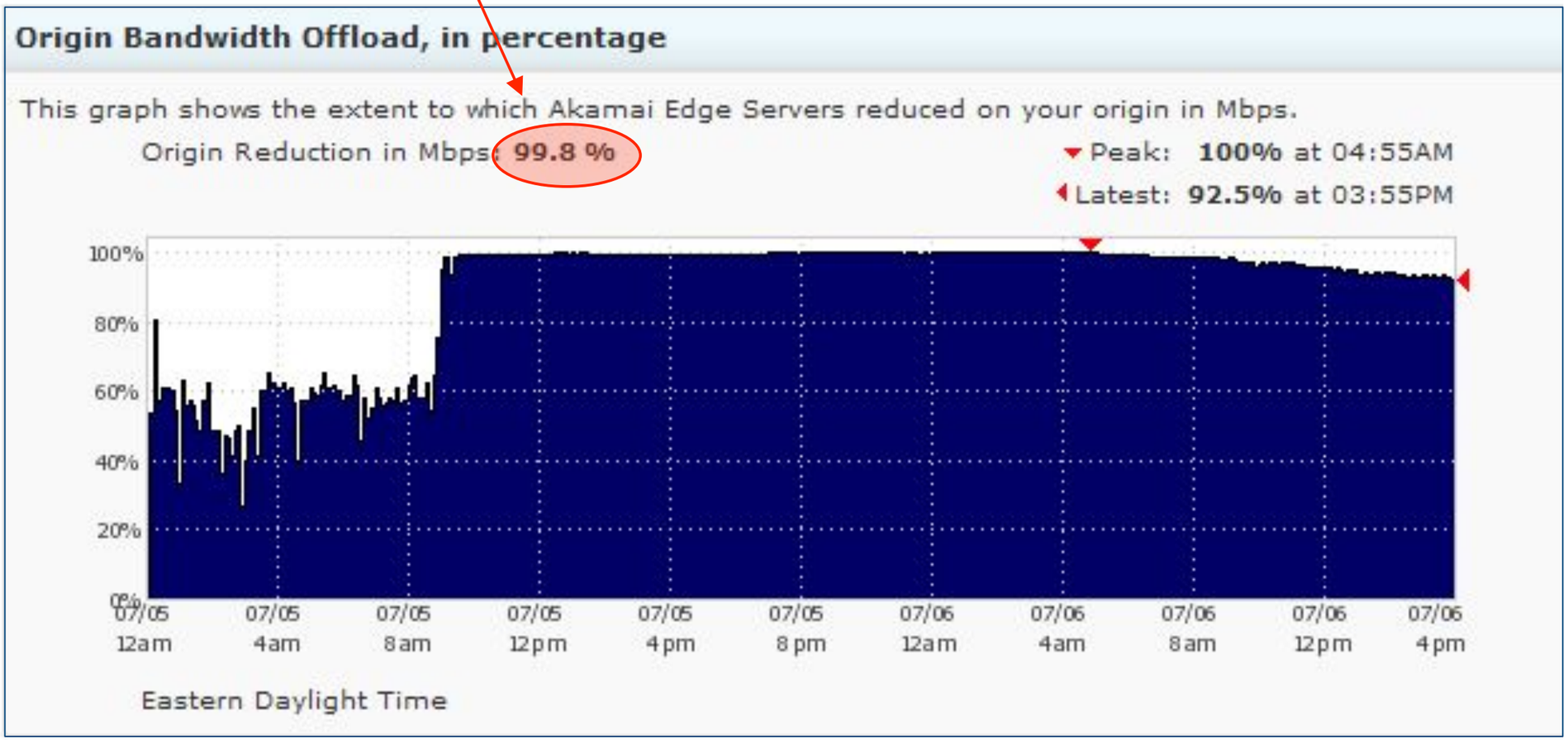
Reducing Risk, Protecting the Brand

- Attack on Akamai stock exchange customer.
- Peak attack traffic was 26 Gbps, 170x normal.
- Page Views peaked at over 260,000 per second, 280x normal.



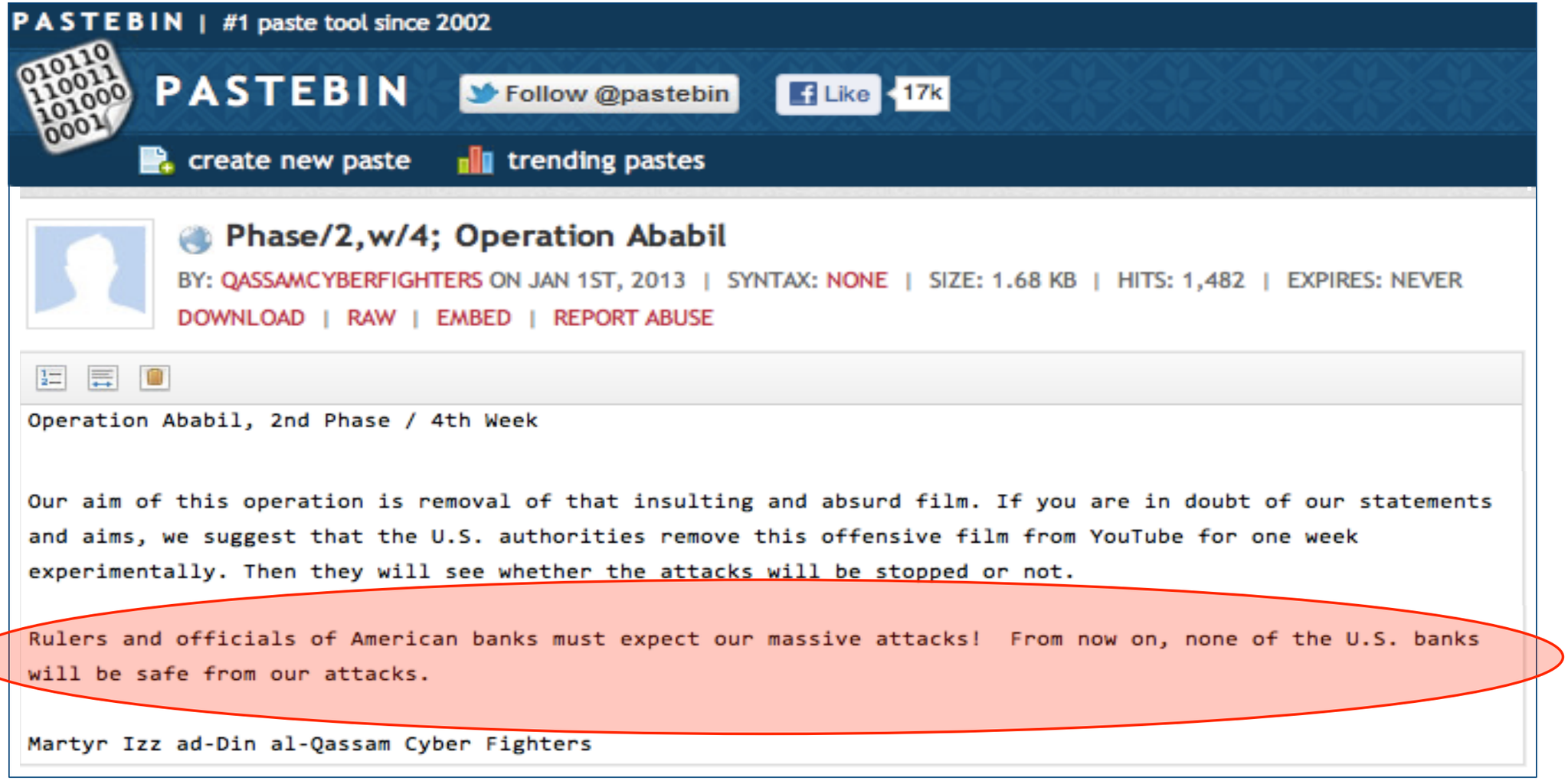
DDoS Attack – Stock Exchange

- Akamai Offloaded over 99% of bandwidth during the attack, protecting the site.
- Origin bandwidth peaked at only 53 Mbps.



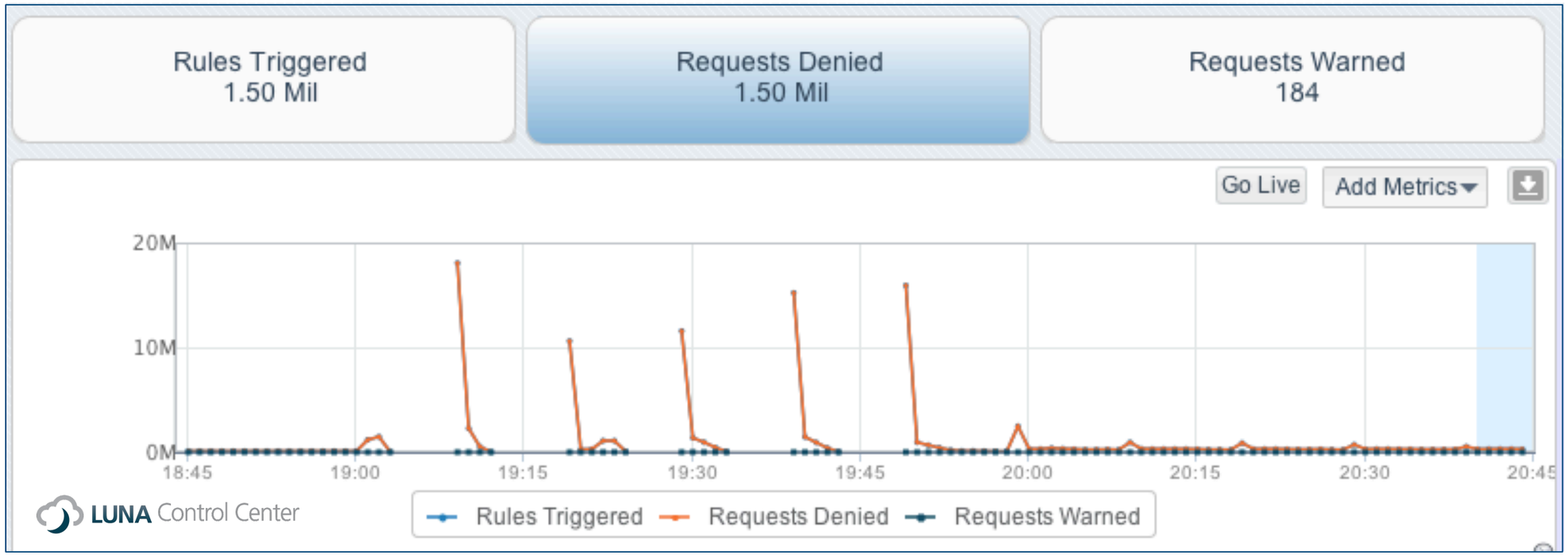
Operation Ababil / 2nd Phase / 4th Week

“none of the U.S banks will be safe from our attacks.”

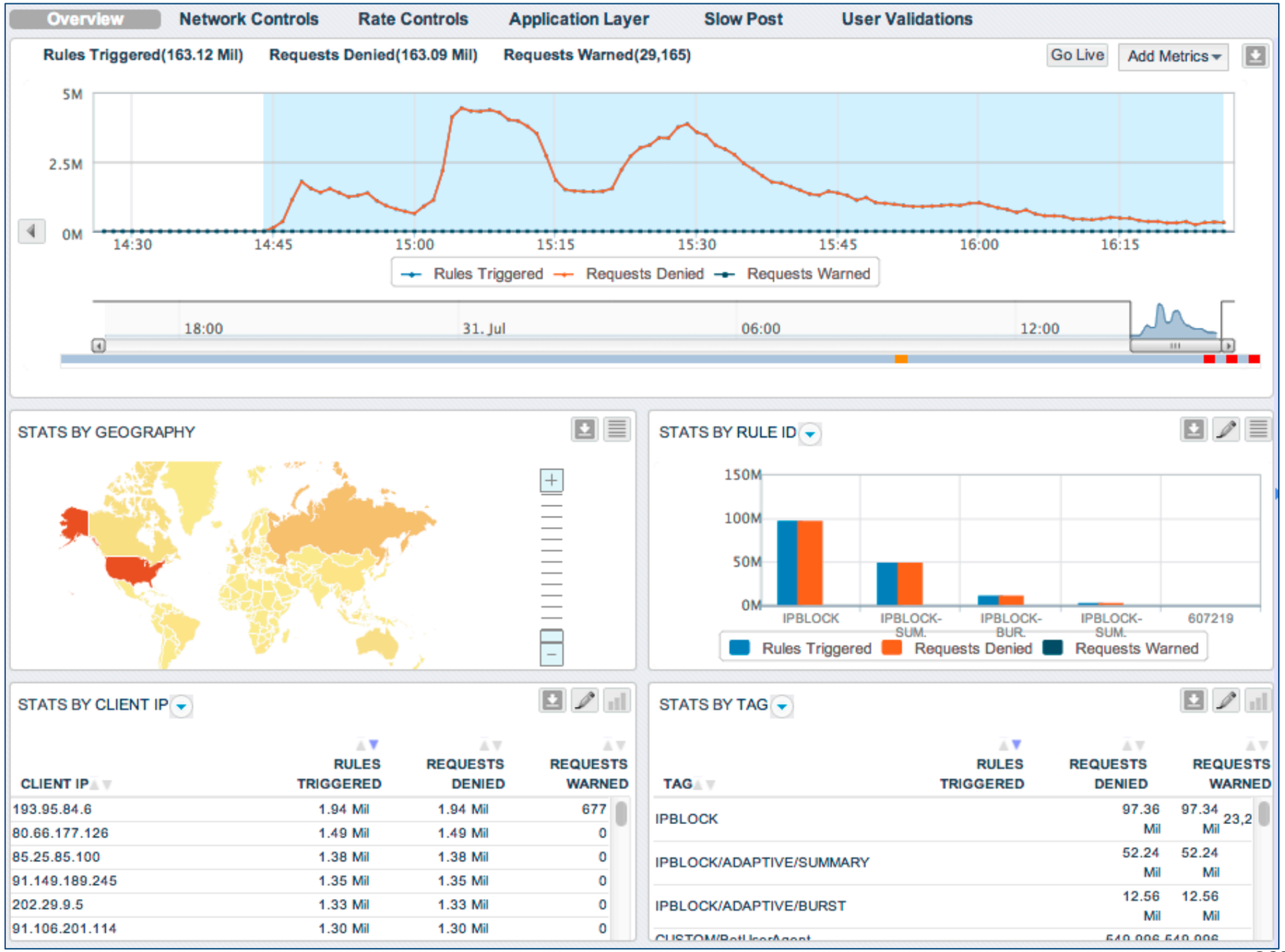


January 10, 2013 – Protect …

- Ababil Phase II. Continued probing against a banking web site.
- Repeated every 10 minutes.
- Peaked at over 18M requests per minute.
- Proof of always-on defense. The target survived the first 40 minutes of attack, and the attackers went to other banks.

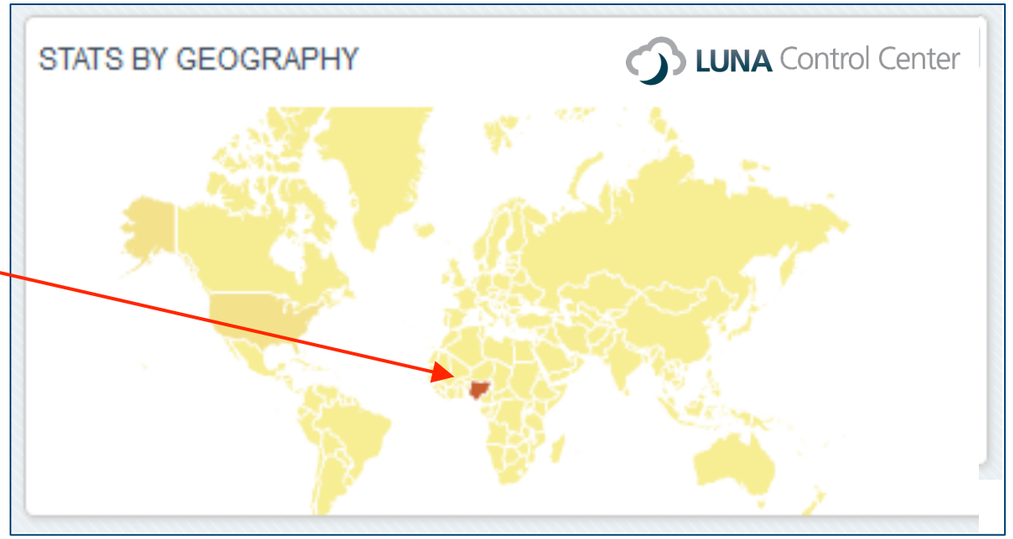


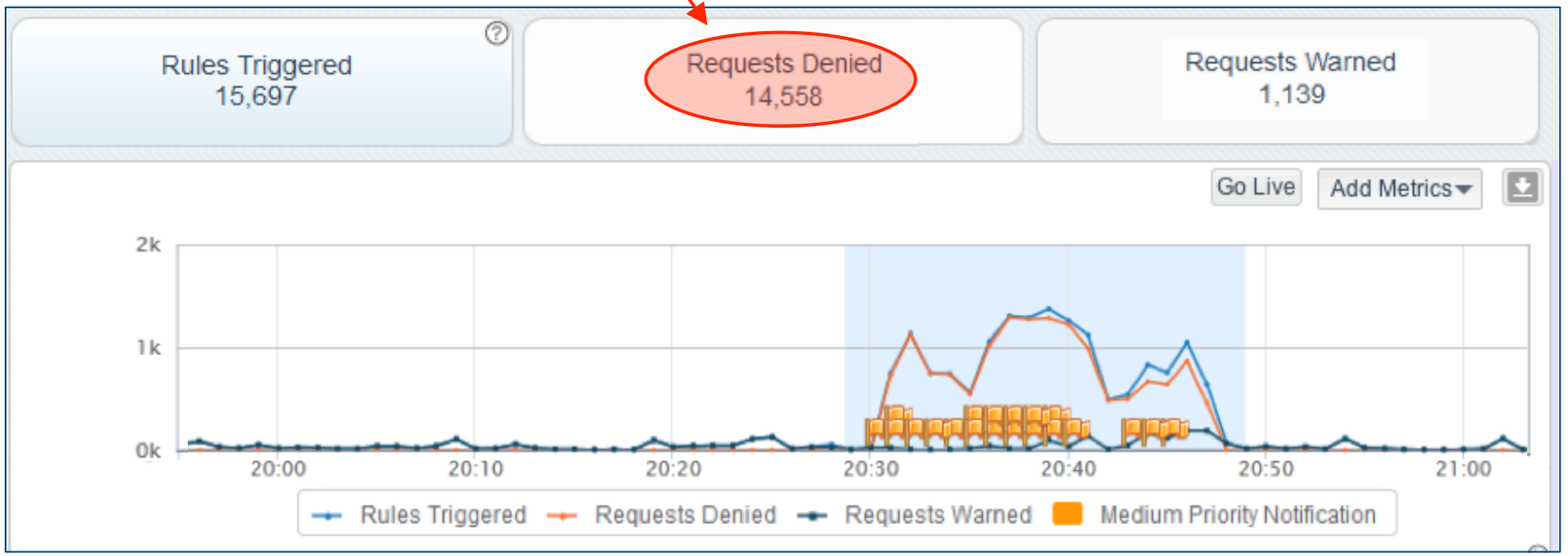
Operation Ababil – Phase 4



Nigerian SQL Injection Attack

- Top financial services firm with over 20M customers.
- Data breach attempt from Nigeria.
- Attack was inside SSL request.
- Over 14,000 attempts blocked by Akamai.





I TRADIZIONALI APPROCCI PER LA DIFESA DAGLI ATTACCHI

- L'attenzione al cambiamento delle minacce di sicurezza - dalla rete alle applicazioni- i disagi per il furto di dati e da attacchi unidimensionali ad attacchi multidimensionali, stanno guidando uno spostamento di architettura nel settore della sicurezza .
- Mentre gli attacchi DDoS e ad applicazioni Web continueranno a richiedere la massima attenzione, molti degli attacchi più dannosi sono anche i più difficili da rilevare, e forniscono poco o nessun preavviso .
- Ciò richiede una postura di sicurezza che sia sempre attiva, ma che garantisca le prestazioni e la scala per rispondere alle più grandi minacce di attacco di rete e a livello applicativo oggi prevalente.

  - On-premises Hardware
  - Internet Service Providers (ISPs)
  - Cloud Security providers

On – premises hardware

- Molte organizzazioni si affidano a dispositivi hardware, come ad esempio firewall di rete, dispositivi per la mitigazione degli attacchi DDoS, ed appliance WAF, dislocati in locali all'interno dei loro data center.

- **Scalabilita'** - Mentre i dispositivi hardware sono sempre in evoluzione, i sistemi di sicurezza basati su hardware possono ancora essere sopraffatti dalla grande quantità di traffico generato dagli attacco botnet di oggi .

- **Prestazioni** - La difesa contro gli attacchi a livello applicativo può essere estremamente onerosa in risorse. Per quando si consideri un approccio basato sull'hardware, è importante ricordare che nessun dispositivo hardware funziona in isolamento.

On – premises hardware (Cont’d)

- Uno svantaggio finale di un approccio hardware-base è che tenta di fermare un attacco DDoS e ad applicazioni Web solo dopo che lo stesso è entrato nel data center. Se un'organizzazione non ha un sufficientemente grande collegamento Internet , allora l'attacco saturerà la larghezza di banda disponibile, causando un'interruzione per tutto il centro dati.

- Anche quando gli attacchi sono difesi con successo, gli attacchi bandwidth-intensive possono degradare le prestazioni per gli utenti legittimi.

- E per come la dimensione degli attacchi DDoS continua a crescere, le organizzazioni dovranno continuare il provisioning di larghezza di banda aggiuntiva per garantire scalabilita’ sufficiente.

Internet Service providers

- Un altro approccio comune per proteggere le applicazioni con accesso a Internet è quello di attuare un servizio attraverso il provider di servizi Internet di un'organizzazione (ISP). Molti ISP offrono servizi di mitigazione DDoS per completare la loro attività principale di fornire la larghezza di banda della rete.

- Questi servizi sfruttano il ruolo e la posizione del provider nella fornitura di traffico di rete tra gli utenti e le applicazioni remote per mitigare gli attacchi DDoS contro le infrastrutture dei propri clienti. Tuttavia, ci sono diverse considerazioni che potrebbero non essere evidente a prima vista:

- ISP multipli - dal punto di vista architettonico, gli ISP possono mitigare solo DDoS traffico attacco in transito sulla loro rete. Molte organizzazioni acquistano banda da più fornitori di servizi Internet al fine di aumentare la disponibilità, migliorare le prestazioni e ridurre i costi di larghezza di banda.

- Scalabilita' - con i più grandi attacchi DDoS superiori a 300 Gbps di larghezza di picco di banda, la maggior parte dei fornitori di servizi Internet semplicemente non ha la capacità di rete sufficiente per mitigare adeguatamente potenziali attacchi diretti ai loro clienti.

- Competenze di Security - la maggior parte degli ISP non considerano la sicurezza come una componente essenziale della loro attività , ma piuttosto una capacità aggiuntiva per aumentare la loro attività principale di fornire la larghezza di banda della rete.

Fornitori di servizi ed infrastrutture di Cloud security

- Le soluzioni di sicurezza cloud-based offrono un nuovo approccio per rilevare e mitigare le minacce alla sicurezza. Qui, le organizzazioni implementano una piattaforma cloud di terze parti di fronte alle loro infrastrutture e in linea tra utenti remoti e le loro siti web e applicazioni. Il fornitore di sicurezza del cloud e' in grado di esaminare il traffico di rete per schermare di attacco noti e passare solo il traffico legittimo attraverso l'applicazione :

- Semplicità - la difesa contro gli attacchi DDoS all'interno del data center richiede il ridimensionamento e la blindatura di molti componenti dell'infrastruttura.

- Scalabilita' - sfruttando le economie di scala che provengono da proteggere molte organizzazioni in una sola volta, il fornitore cloud può costruire una infrastruttura molto più grande di quello che le singole organizzazioni possono costruire e gestire da soli.

- Prestazioni - alcune soluzioni di sicurezza cloud-based sono in grado di migliorare le prestazioni, proteggendo le applicazioni contro DDoS e attacchi alle applicazioni Web.

- Threat intelligence – I fornitori di sicurezza di cloud in genere hanno una maggiore visibilità degli attacchi e delle tendenze di attacco per le singole organizzazioni. A causa della loro posizione nella rete, si può vedere un attacco come sua prima utilizzazione contro uno dei loro clienti e quindi sfruttare le tecnologie e le tecniche utilizzate per la difesa contro questo attacco per migliorare la sicurezza di altri clienti.

Fornitori di servizi ed infrastrutture di Cloud security (Cont'd)

- Competenza - l'efficacia delle capacità di qualsiasi organizzazione per rispondere ai DDoS o ad attacchi alle applicazioni Web è fortemente influenzato dalla sua esperienza a mitigare altri attacchi simili. Con la difesa contro gli attacchi diretti a molte organizzazioni individuali nel corso del tempo, il cloud provider di protezione e' in grado di sviluppare competenze ed esperienze significative. Essi possono trarre da questa esperienza quando mitigare attacchi futuri per ridurre i tempi di mitigazione e alcun impatto sui loro clienti.

- Compliance - molte organizzazioni con operano siti web e applicazioni che sono soggetti a diverse disposizioni di legge, come la Payment Card Industry Data Security Standard (PCI DSS) per qualsiasi sito che gestisce le informazioni della carta di credito. Le organizzazioni devono garantire che la loro soluzione di sicurezza cloud rispetta anche tutte le norme di legge applicabili a cui sono sottoposti.

- Costi - con una soluzione di sicurezza basata su cloud, le organizzazioni possono operare una spesa capitale iniziale con una spesa operativa ricorrente molto più bassa, considerando le dimensioni dell'infrastruttura da proteggere.

LA NECESSITA’ DI UNA DIFESA PROATTIVA

- In termini semplici , la sicurezza web gestita è costituita da servizi in outsourcing studiati appositamente per dare alle imprese on-line una difesa proattiva contro le violazioni dei dati , attacchi DDoS , e la completa attuazione delle difese per una continua evoluzione delle minacce informatiche emergenti.

- Esperti della sicurezza Web sulla squadra di sicurezza del provider Cloud non solo sono in grado di rilevare e mitigare gli attacchi , ma anche agire come consulenti per la sicurezza Web, che assicurano che le applicazioni Web e sistemi di rete sono sempre up-to -date e protetti contro le minacce emergenti .

- I servizi di sicurezza web gestiti concentrano idealmente sulla fornitura di più strati di protezione dalle minacce.

Rilevamento, monitoraggio e mitigazione interattiva delle minacce

- La diagnosi precoce e la mitigazione immediata di attacchi informatici sono i tratti distintivi di un servizio di sicurezza web best-in-class gestito e di una difesa proattiva contro le minacce basate su Internet.
- Perché è la diagnosi precoce è così importante? Il tempo è letteralmente denaro quando mitigare un attacco DDoS, violazione dei dati o altro tipo di cyber-attacco.
- Secondo una relazione di maggio 2013, analista di Forrester John Kindervag, una società di servizi finanziari ha registrato $ 17 milioni di perdita stimata per un incidente DDoS nel 2012.
- L'impatto finanziario stimato -di attacco DDoS- è stato di $ 2,1 milioni di dollari persi per ogni 4 ore di inattività e di $ 27 milioni di dollari per una interruzione di 24 ore.
- Queste cifre possono essere estrapolate al di là del settore dei servizi finanziari da applicare a qualsiasi industria, governo o organizzazione che fa affari o fornisce applicazioni via Web.

Manutenzione attiva e assistenza nella configurazione delle Web Apps

- Le applicazioni Web sono facile preda di attacchi informatici e spesso aprono la porta per violazioni dei dati e il furto di dati personali (PII). Gli aggressori cercano gli anelli più deboli per cercare di ingannare l'applicazione Web a rivelare i dati in ogni modo possibile.

- Le applicazioni Web che hanno regole datate e sono out-of-date sono in genere più vulnerabili e rappresentano il maggior rischio per consentire l'accesso ai malintenzionati.

- All'interno di una soluzione di sicurezza Web gestita, i clienti possono aumentare la migliore pratica di un ciclo di vita di manutenzione software sicuro con una soluzione Web di Application Firewall (WAF) gestita dal fornitore di servizi e dai consigli degli esperti del SOC.

- Perchè il mantenimento attivo di applicazioni Web è così importante: i clienti Akamai hanno segnalato 768 attacchi a livello applicativo nel 2014 e 1153 nel 2015, un anno aumento del 50 per cento anno su anno.

- VeraCode prevede che tre su quattro aziende saranno obiettivo ad un certo punto da exploit di applicazioni Web e che le applicazioni Web rappresenteranno il 54 per cento di tutte le violazioni dei dati a base di hacking.

Revisione strategica delle configurazioni di sicurezza web

- La maggior parte delle organizzazioni non hanno risorse IT con l'esperienza necessaria per mantenere e ottimizzare le configurazioni di sicurezza web.
- Una tipica azienda richiederebbe almeno tre dipendenti IT a tempo pieno per fornire una copertura 24/7, più gli straordinari nei fine settimana, per round-the-clock, operazioni di sicurezza web in-house.
- Nonostante considerazioni di costo è molto difficile da trovare e mantenere i talenti IT con questo livello di competenze sulla sicurezza web specializzati con l'esperienza nella configurazione di tali sistemi.
- I fornitori di servizi di sicurezza gestita web consentono la sfida aiutando le organizzazioni a rimanere pienamente preparate per i futuri attacchi informatici.
- Regolari revisioni strategiche della configurazione di sicurezza web da parte di esperti SOC assicurano che la soluzione è sempre messo a punto, up-to-date, e pronti a difendere contro le ultime vettori di attacco e toolkit.
- Un fornitore di servizi di sicurezza web gestita può anche fornire altre raccomandazioni di esperti su regole personalizzate e aggiornamenti di set di regole che assicurino la migliore protezione per il business.

LA AKAMAI INTELLIGENT PLATFORM

- Akamai offre una soluzione sempre attiva di sicurezza cloud sulla base della nostra Akamai Intelligent Platform . Originariamente fondato come la piu' grande CDN, la piattaforma intelligente di Akamai è evoluta al di là dell'accelerazione dei contenuti per garantire la sicurezza della rete e a livello di applicazione per i siti web e altre applicazioni Internet. La sua scala globale e la connettività offre diversi vantaggi intrinseci quando difende contro molte delle minacce alla sicurezza più diffuse di oggi .

- Un'architettura naturale per la sicurezza Web

- Come una soluzione di sicurezza cloud-based, la piattaforma intelligente di Akamai si poggia di fronte a siti web e altre applicazioni Internet, gestendo il traffico delle applicazioni di rete dagli utenti alle applicazioni e contenuti dalle applicazioni viceversa verso gli utenti . La sua architettura distribuita e sempre attiva offre due vantaggi per la difesa contro gli attacchi di rete e di livello applicativo:

LA AKAMAI INTELLIGENT PLATFORM (Cont'd)

Inline - L'architettura in linea offre una posizione natural, da cui difendersi contro qualsiasi tipo di DDoS o da attacchi ad applicazioni web. Poiché il traffico passa attraverso l' Akamai Intelligent Platform verso l'applicazione, la piattaforma in grado di identificare e analizzare gli attacchi, così come intraprendere le azioni appropriate per mitigarli. Inoltre la sua architettura in linea consente alla Intelligent Platform di Akamai di applicare modelli di sicurezza sia positivi che negativi a seconda dei casi per una maggiore flessibilità.

Distribuita - Gli utenti accedono a siti web e ad altre applicazioni Internet mediante le risorse distribuite a livello globale della Akamai Intelligent Platform, tra cui oltre 210.000 server perimetrali e sette DDoS scrubbing center a livello mondiale. Ciò fornisce una piattaforma distribuita per la protezione delle applicazioni con accesso a Internet, con molti punti della rete in cui possono essere eseguite le attività di mitigazione.

La Akamai Intelligent platform: chi e' Akamai?

A Global Company

- 6,100+ employees
- $ 2.3B Revenue (2015)
- 52+ offices worldwide
- S&P 500 and NASDAQ 100

A Global Platform

- 210,000+ Servers
- 7 DDoS dedicated scrubbing centers
- 1,300+ Networks
- 100+ Countries

Delivering 130,000+ Domains

- Over 100 banks worldwide
- All top 60 eCommerce sites
- All top 30 M&E companies
- All of the top Internet portals

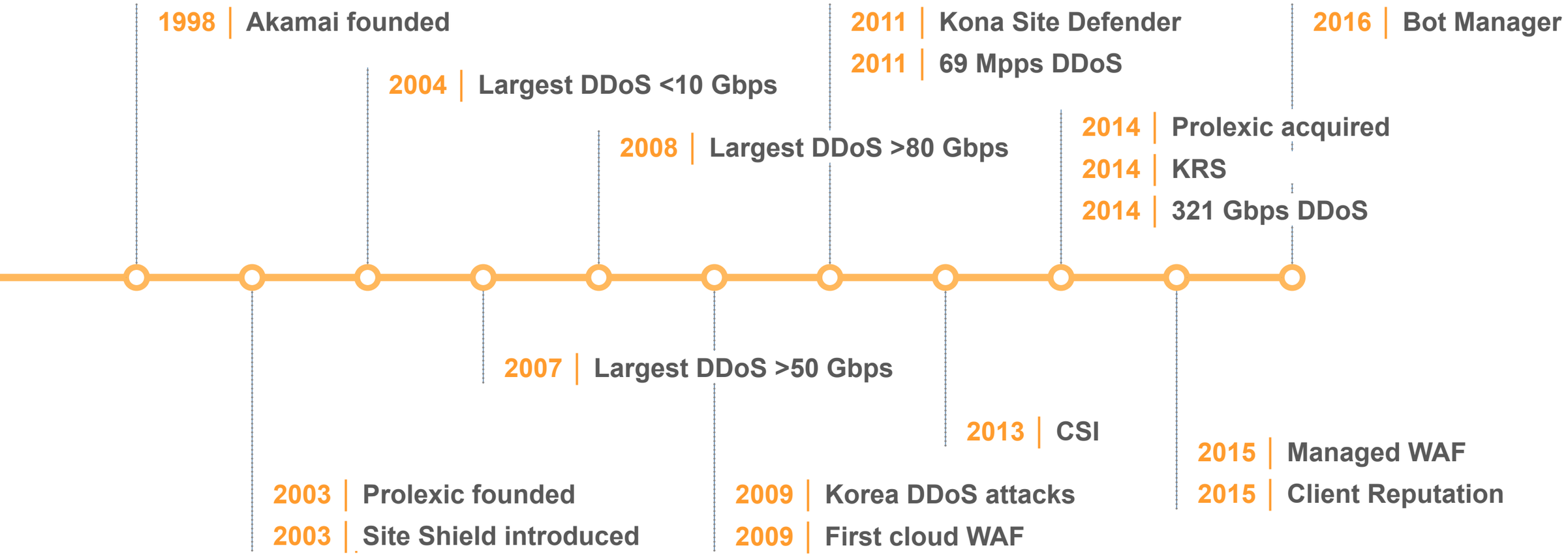
Accelerating Daily Traffic of

- 25+ Tbps
- 19+ million hits per second
- 2+ trillion deliveries/day
- 30+ petabytes/day

Handling 15 – 30+% of daily Web Traffic

Helping secure web applications for

OVER 18 YEARS



Le maggiori aziende del settore Finance hanno scelto Akamai

- All top 10 banks (Source: The Banker)
- All top 10 asset managers (Source: Towers Watson)
- All top 10 P&C insurance carriers (Source: A.M. Best)
- 7 of the top 10 Life & Health carriers (Source: A.M. Best)
- 9 of the top 10 FinTech companies (Source: American Banker)
- Top firms in Cards & Payments, Financial Information Services, Brokerage, and Forex
- Over 100 banks worldwide use Akamai security solutions

Over $1 Trillion in financial transactions annually are executed on the Akamai Intelligent Platform.

Come opera l'Akamai Security Platform

DDoS scrubbing centers close to the IP origin

High Performance Global Overlay Network

Application Server & Data Centers

Edge Region close to Origin Server

Edge Region or Scrubbing Center close to IP origin

Customers

Web Applications
Mobile Applications
IP Applications
& Data Centers

Cybercrime

"SureRoute" and Akamai Protocol optimize route and reduce round trips

Security embedded into Akamai Edge Servers

Cloud security Intelligence framework (CSI)

Come opera l'Akamai Security Platform

DDoS scrubbing centers close to the IP origin

High Performance Global Overlay Network

Application Server & Data Centers

Edge Region close to Origin Server

Edge Region or Scrubbing Center close to IP origin

Customers

Web Applications
Mobile Applications
IP Applications
& Data Centers

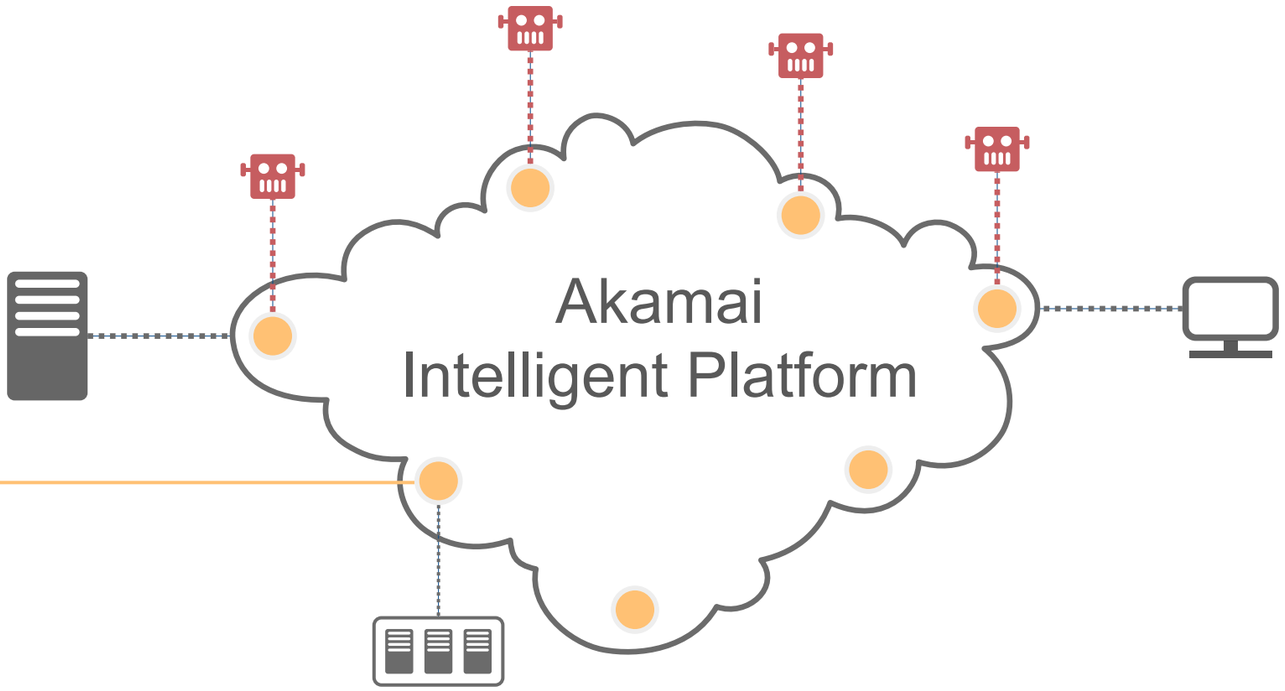
"SureRoute" and Akamai Protocol optimize route and reduce round trips

Security embedded into Akamai Edge Servers

Cybercrime

Cloud security Intelligence framework (CSI)

Cloud Security Intelligence



Visibility | 15-30% of global web traffic | every Akamai customer

Data | 80 million WAF triggers per hour | 600,000 log lines a second | 20 TB new attack data daily

Analysis | dedicated threat research team | 8,000 queries a day

Migliorare la sicurezza con informazioni aggiornate sulle minacce

La sofisticazione e la complessità degli attacchi sono in aumento ogni giorno, come gli hacker sviluppano nuovi strumenti e scoprono nuove vulnerabilità da sfruttare. Grazie alla scala globale della piattaforma intelligente di Akamai, Akamai ha una visibilità senza pari in attacchi contro le piu' grandi, più trafficate, e più frequentemente attaccate proprietà e marchi online, ed utilizza questa visibilità in diversi modi:

1. Per Individuare nuove tendenze di attacco come si sviluppano o di nuovi vettori di attacco che non sono mai stati utilizzati prima.

2. Per avvertire proattivamente i clienti del rischio di una minaccia emergente o per regolare la configurazione di sicurezza dei siti web protette e altre applicazioni Internet.

3. Per sviluppare regole WAF per mitigare i vettori di attacco di recente scoperta, o perfezionare quelli esistenti per migliorare la precisione della nostra protezione contro gli attacchi alle applicazioni web.

4. Per migliorare gli strumenti e processi utilizzati dai SOC globali di Akamai per rilevare, identificare e mitigare gli attacchi futuri in modo più rapido ed efficace.

5. Per pubblicare specifici bollettini sulle minacce per i clienti attraverso i servizi di intelligence sulle minacce di Akamai.

CONCLUSIONI

- Con Akamai , le organizzazioni possono scaricare il fabbisogno di distribuzione di risorse di una infrastruttura di sicurezza fisica globale e concentrarsi invece su come personalizzarle per soddisfare le esigenze di sicurezza del loro business.

- La piattaforma intelligente di Akamai si adatta anche per il panorama delle minacce che cambia, con i team di sicurezza di Akamai in costante sviluppo e pubblicazione di nuove regole e processi di sicurezza in risposta alle minacce più recenti.

- Akamai ha investito nella costruzione di relazioni all'interno della comunità di sicurezza, come ad esempio con OWASP , FS – ISAC, Nanog, e con governi e forze dell'ordine. Akamai combina queste intelligenze esterna con i dati sulle minacce messi a disposizione dalla piattaforma Intelligente di Akamai per semplificare la messa in sicurezza delle singole organizzazioni.

CONCLUSIONI (Cont'd)

Le tecnologia di sicurezza di rete da sole, seppur vitali, non possono adeguatamente fermare gli attacchi da mutevoli toolkit e vettori di attacco innovativi da parte di sofisticati criminali informatici.

- Un servizio di sicurezza web gestito è una parte essenziale di una difesa sicurezza online proattiva che contrappone i tecnici di grande esperienza del SOC ed apparati state-of-the-art contro gli attacchi cibernetici.

- Akamai sostiene che i servizi di sicurezza web gestiti insieme con i migliori sistemi di monitoraggio degli attacchi e le migliori tecnologie di mitigazione in un approccio multi-livello rappresentano il modo migliore, più efficace e più proattivo per combattere e vincere contro le minacce informatiche, oggi e nel futuro.

THANK YOU !

Paolo Bufarini - Head of Security, Italy and Mediterranean Region, Akamai