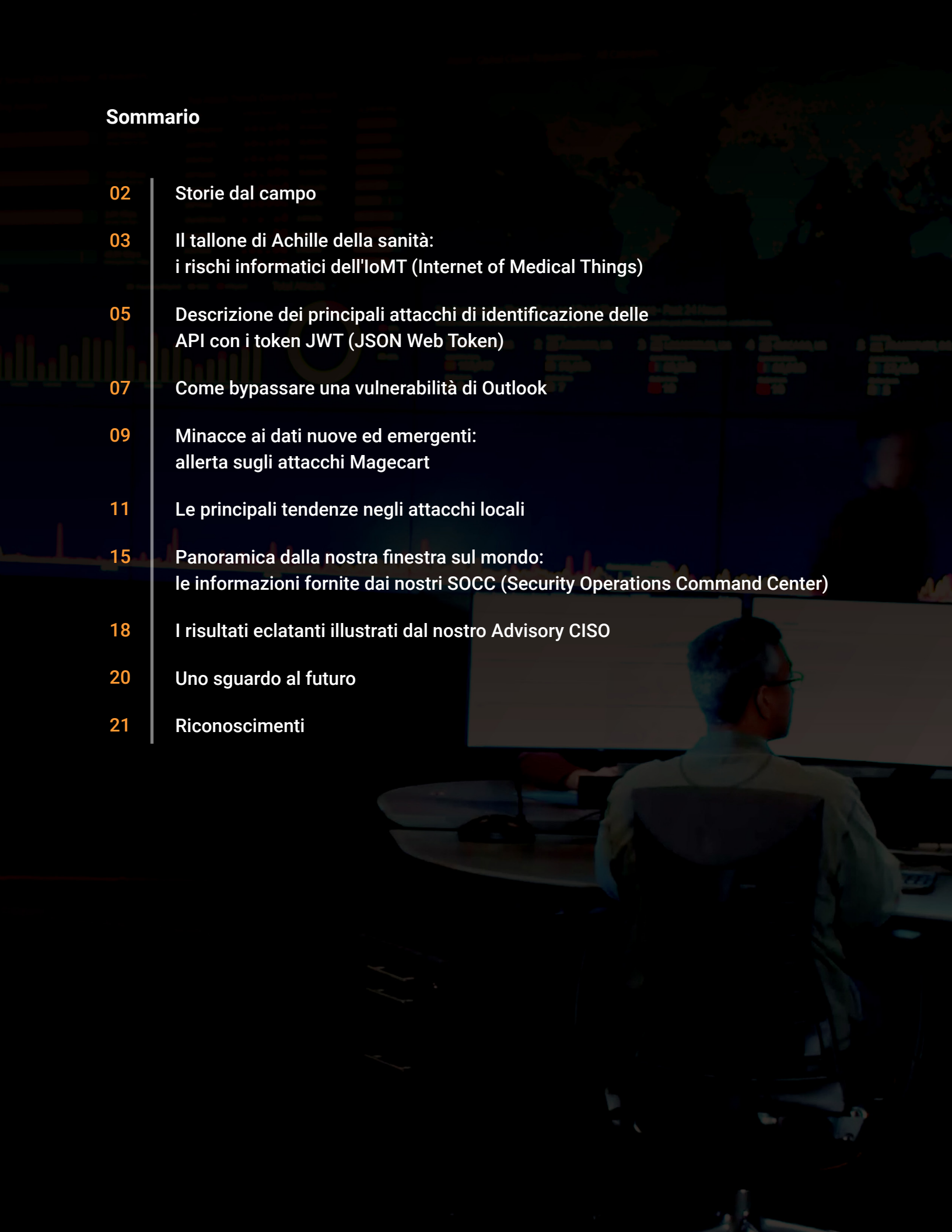
Akamai
Stato di Internet
Volume 9 | Numero 6

Esame dell'anno

Uno sguardo sulle tendenze per la cybersicurezza nel 2023 e su cosa aspettarsi per il futuro

Sommario



Storie dal campo

Per questo rapporto sullo stato di Internet (SOTI), ci siamo distaccati dal consueto esame dell'anno in cui vengono rivisti tutti i precedenti rapporti che abbiamo pubblicato quest'anno per focalizzarci invece su questo tema fondamentale: Qual è la vostra storia dell'anno riguardo alla sicurezza? Abbiamo chiesto ad alcuni redattori e analisti di dati del SIG (Security Intelligence Group) di Akamai di stilare una valutazione annuale delle storie di cui abbiamo trattato negli ultimi 10 mesi. Non deve essere stato un compito facile per loro scegliere solo una storia tra le tante interessanti vicende e tra le nuove scoperte di cui abbiamo trattato nel nostro blog per la ricerca sulla sicurezza e nei rapporti SOTI pubblicati nel 2023. Abbiamo anche chiesto al nostro Advisory CISO e ad un vicepresidente dei nostri SOCC (Security Operations Command Center) di valutare le tendenze osservate negli attacchi di quest'anno e le principali lezioni apprese di cui dobbiamo tener conto nel 2024.

Tante cose sono accadute quest'anno nel campo della sicurezza e nell'ambito del team Akamai Security Research. I contributi offerti alla ricerca dai nostri esperti di sicurezza sono indubbiamente preziosi per la comunità. Tramite il nostro hub dedicato, i professionisti della sicurezza possono accedere facilmente a risorse affidabili contenenti informazioni, strategie di mitigazione e tendenze degli attacchi che possono aiutarli a difendere le loro organizzazioni. Inoltre, possono accedere a strumenti gratuiti, come il nostro kit di strumenti RPC e Infection Monkey, la nostra piattaforma di emulazione delle attività dei criminali open source. Agendo proprio come il malware, la piattaforma Infection Monkey propaga e "crittografa" i file a cui può accedere stravolgendo le regole tradizionali, ossia fornendo al professionista della sicurezza una visione realistica di come un criminale potrebbe (o non potrebbe) spostarsi in quell'ambiente. La velocità con cui si evolvono le minacce rende necessaria l'esecuzione di test continui. I professionisti della sicurezza devono conoscere la situazione della loro rete oggi, non solo durante l'ultimo test di penetrazione.

Se potessimo riassumere in una parola lo scenario del 2023, potremmo usare il termine *svolta*. I criminali hanno cambiato la loro tattiche per eludere le misure di sicurezza alla ricerca di nuove superfici di attacco e di obiettivi mai presi di mira per creare scompiglio nelle organizzazioni di tutte le dimensioni e di ogni settore. Lo stesso si potrebbe dire per gli addetti alla sicurezza che continuano a ricalibrare i loro metodi e a cercare nuovi modi per mitigare gli attacchi e proteggere meglio le organizzazioni. La nostra svolta si realizza tramite soluzioni, ricerche e strumenti con questo obiettivo: fornire preziose informazioni e strategie di mitigazione ai professionisti della sicurezza che lottano contro le nostre stesse minacce.

Buona lettura!

Il tallone di Achille della sanità: i rischi informatici dell'IoMT (Internet of Medical Things)

Mi chiamo Badette Tribbey e mi occupo della stesura dei rapporti SOTI. Collaboro con gli esperti della sicurezza e gli analisti di dati per trasformare i risultati e i dati tecnici in informazioni utili. Odio la matematica, ma mi piace il modo con cui i numeri possono rivelare interessanti tendenze degli attacchi.

Uno degli argomenti principali che abbiamo trattato quest'anno ci tocca da vicino: i maggiori rischi introdotti dall'IoMT (Internet of Medical Things). Nei due rapporti Sfruttare le falle nella sicurezza e Il ransomware in azione, abbiamo esaminato i rischi osservati nel settore scientifico-sanitario e le caratteristiche che lo rendono vulnerabile agli attacchi. Uno degli aspetti che mi ha colpito maggiormente è il modo con cui le risorse dell'IoMT, come le apparecchiature per la risonanza magnetica, le pompe insuliniche e i dispositivi indossabili, anche se estremamente vantaggiosi per i pazienti, abbiano aumentato notevolmente i rischi per le strutture sanitarie. Queste organizzazioni stavano già affrontando le sfide correlate con la protezione del loro perimetro a causa della complessità dell'ecosistema sanitario, della vulnerabilità della tecnologia tradizionale e dei problemi del personale IT e degli addetti alla cybersicurezza. Inoltre, un'applicazione tempestiva delle patch in questo ambiente può risultare un lavoro sovrumano, con aggiornamenti forniti da vari vendor per più sistemi o applicazioni, di cui è, pertanto, difficile tenerne traccia.

I dispositivi IoMT privi di patch sono tra le risorse più vulnerabili di tutti i settori e possono introdurre minacce ancora più nefaste, come i ransomware. Poiché l'IoMT cresce in modo esponenziale (insieme all'utilizzo delle API), aumentano anche le relative vulnerabilità, che possono fornire ai criminali un punto d'appoggio nei sistemi presi di mira o venire sfruttate causando una fuga di dati (Figura 1). Un rapporto congiunto stilato da Cynerio e dal Ponemon Institute e relativo ad uno studio condotto su vari ospedali e sistemi sanitari negli Stati Uniti ha rivelato che più della metà di queste strutture ha subito attacchi informatici a causa delle falle di sicurezza presenti nei dispositivi IoMT.

> “Un'applicazione tempestiva delle patch in questo ambiente [nel settore sanitario] può risultare un lavoro sovrumano, con aggiornamenti forniti da vari vendor per più sistemi o applicazioni, di cui è, pertanto, difficile tenerne traccia.
>
> **- Badette Tribbey, Senior Technical Writer, Akamai**

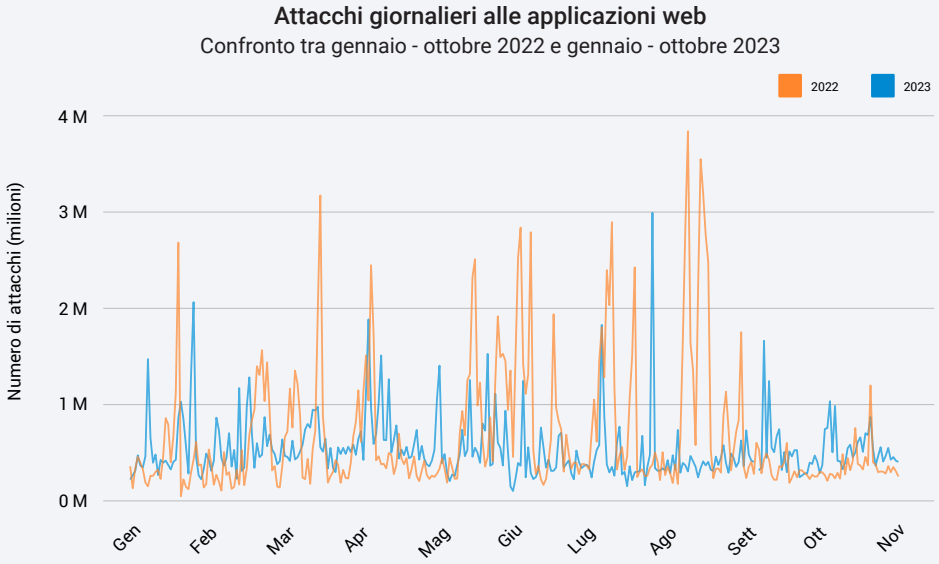


Figura 1. Gli attacchi alle applicazioni web e alle API nel settore farmaceutico-sanitario rimangono stabili con alcuni sporadici picchi registrati tra il 2022 e il 2023. Anche se gli attacchi sono diminuiti del 21% su base annua, il numero medio di attacchi al giorno nel 2023 è più alto rispetto al 2022.

Cosa aspettarsi nel settore sanitario?

Considerando l'aumento del numero di dispositivi IoMT nel settore sanitario, le API continueranno a svolgere un ruolo cruciale nella facilità di accesso ai servizi medici (ad es., la telemedicina e il monitoraggio remoto dei pazienti), migliorando così i risultati clinici e finanziari. Inoltre, è probabile che gli attacchi contro il settore sanitario non diminuiranno a causa dell'elevato valore delle cartelle cliniche e dei dati dei pazienti sul dark web.

Spostando la nostra attenzione dall'oggi al domani, è chiaro che i criminali continueranno ad innovarsi e ad aumentare l'ambito e la complessità dei loro attacchi. Probabilmente, vedremo continuare ad aumentare il numero di attacchi più tecnici che sfruttano le vulnerabilità zero-day. Inoltre, poiché sta cambiando lo scenario delle normative, tra cui il [PATCH] (Protecting and Transforming Cyber Health Care) Act del 2022, dobbiamo garantire che le nostre soluzioni siano in grado di aiutare a soddisfare la conformità richiesta dalle incombenti leggi in materia di privacy, creazione di rapporti, pagamenti, sovranità dei dati e resilienza. Infine, prevediamo di registrare ulteriori problemi a seguito degli attacchi sferrati contro aziende i cui CISO spostano i loro budget per consolidarli su un minor numero di vendor e per utilizzare soluzioni in grado di ridurre al minimo il tempo di permanenza degli hacker che sono penetrati nei loro sistemi.

Descrizione dei principali attacchi di identificazione delle API con i token JWT (JSON Web Token)

Mi chiamo Lance Rhodes e svolgo con passione il ruolo di Cybersecurity Writer nel team Akamai SIG da marzo 2023! Gran parte del mio lavoro serve da "tessuto connettivo" tra i nostri rapporti e i blog poiché lavoro sia sugli aspetti editoriali che sulla stesura dei blog e delle ricerche locali, nonché sulla stesura dei contenuti e dei materiali di marketing per i rapporti SOTI. Tutti questi contenuti vengono poi collegati grazie alla mia collaborazione con il team nelle nostre newsletter interne ed esterne e nei rapporti relativi alle conferenze sulla sicurezza.

Devo dire che uno dei blog più interessanti su cui ho lavorato quest'anno è stato quello sui token JWT (JSON Web Token). Questo post era direttamente correlato al rapporto SOTI sulle app e sulle API (Sfruttare le falle nella sicurezza) nel senso che trattava più in dettaglio la violazione dell'autenticazione nei token JWT (JSON Web Token), uno dei metodi standard di identificazione delle API. Pertanto, ho trovato molto interessante approfondire meglio i token JWT.

Dopo aver lavorato al rapporto SOTI sulle app e sulle API all'inizio di quest'anno, ho iniziato a collaborare con Nitzan Namer per il post sui token JWT, che sono stati descritti come un vettore di attacco per la violazione dell'autenticazione dell'utente, una delle 10 principali vulnerabilità per la sicurezza delle API riportate nell'elenco OWASP (Open Web Application Security Project). Il rapporto SOTI presentava una specifica sezione dedicata a quest'argomento, ma il blog ha analizzato più in dettaglio la struttura dei token JWT e le best practice consigliate per proteggersi dalle principali minacce, tra cui l'escalation dei privilegi, la fuga di dati e il controllo degli account.

Ricordo di aver parlato con Nitzan circa il modo con cui speravamo che il post venisse utilizzato, ossia come risorsa continua per ricercatori della sicurezza, esperti tecnici e utenti/amministratori dei token JWT. Il post ha soddisfatto le nostre aspettative nel suo stile strutturale: sono state elencate prima gli elementi basilari dei token JWT, seguiti da sei casi di utilizzo, che hanno incluso illustrazioni esemplificative di alcune minacce comuni con le relative best practice per ciascuna di esse. L'elenco degli elementi basilari ha fornito informazioni su come i JWT proteggono le API tramite l'emissione di token contenenti informazioni da condividere come oggetti JSON. Pur non essendo crittografato, ogni token è codificato e dotato di un'intestazione, un payload e una firma di verifica (con la quale si attesta che i dati non sono stati alterati quando il server ha creato il token).

> “Il blog ha analizzato più in dettaglio la struttura dei token JWT e le best practice consigliate per proteggersi dalle principali minacce, tra cui l'escalation dei privilegi, la fuga di dati e il controllo degli account.
>
> **- Lance Rhodes, Cybersecurity Writer, Akamai**

I sei casi di utilizzo sono:

1. Uso di token senza convalida da parte dei server
2. Uso della stessa chiave privata per applicazioni diverse.
3. Uso di un algoritmo di firma debole
4. Scelta di una chiave privata corta e/o a bassa entropia
5. Conservazione dei dati sensibili nel payload di un JWT
6. Scambio delle chiavi

I JWT sono uno dei formati di verifica più comuni. L'adozione di appropriate misure di sicurezza è cruciale poiché il formato offre una vasta superficie di attacco che lascia ampio spazio agli errori. Sebbene questi casi di utilizzo mostrino alcune delle più comuni minacce ai JWT, ce ne sono molte altre in circolazione e le tecniche di attacco si evolvono in continuazione.

I JWT non sono crittografati né implementati per motivi di sicurezza

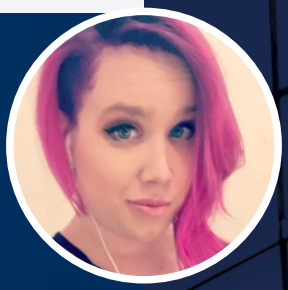
Uno dei principali insegnamenti che ho appreso da questo blog consiste nel fatto che i JWT non sono crittografati né implementati per motivi di sicurezza. È difficile credere che un token di autenticazione comune possa risultare così vulnerabile. In parte, i JWT risultano allettanti perché consentono l'utilizzo di molte applicazioni web e API senza dover effettuare in continuazione l'accesso. Sia il rapporto SOTI che il blog sui JWT hanno analizzato gli algoritmi dei JWT nel traffico di Akamai e hanno stabilito che gli algoritmi simmetrici sono i più comuni, anche se teoricamente sono meno sicuri e non garantiscono lo stesso livello di protezione degli algoritmi asimmetrici. Ad esempio, entrambe le pubblicazioni mostrano che il 54,8% dei clienti di Akamai utilizza l'algoritmo HS256, che è di tipo simmetrico.

È probabile che gli algoritmi simmetrici vengano scelti più spesso perché l'utente ha bisogno solo di una chiave, mentre gli algoritmi asimmetrici richiedono molte più risorse computazionali. La crittografia JWE (JSON Web Encryption), ossia la versione crittografata dei token JWT, non è comunemente utilizzata. La maggior parte delle aziende sceglie i token JWT per risparmiare in termini di potenza di elaborazione.

Conclusione: praticità, costi ridotti e velocità sono caratteristiche spesso considerate prioritarie rispetto alla sicurezza. Questo importante promemoria ci ricorda l'importanza del nostro lavoro di redattori e ricercatori della sicurezza. Le buone pratiche e un'attenta ricerca della sicurezza sono necessarie per trovare il giusto equilibrio tra efficienza e protezione.

> È difficile credere che un token di autenticazione comune possa risultare così vulnerabile.
>
> - Lance Rhodes, Cybersecurity Writer, Akamai

Come bypassare una vulnerabilità di Outlook



Salve, spero che la giornata di oggi vi sorrida! Mi chiamo Tricia Howard e mi occupo dei blog del SIG. Vivo nel concreto mondo degli articoli tecnici e collaboro con i nostri ricercatori, il nostro team addetto alle comunicazioni aziendali e il nostro reparto legale, tra gli altri, per raccogliere informazioni in modo tempestivo ed efficace. La parte migliore del mio lavoro è che posso vantarmi per i meriti dei nostri ricercatori perché fanno davvero cose fantastiche!

Tra tutte le cose su cui mi è stato chiesto di scrivere quest'anno, questa potrebbe essere la più difficile. Tra tutte le cose straordinarie che il nostro team ha fatto negli ultimi 12 mesi, come potrei mai sceglierne solo una? Ma siccome devo farlo, sceglierò il lavoro di Ben Barnea sul famigerato argomento Come bypassare una vulnerabilità di Outlook. Ben, uno dei ricercatori più brillanti che io conosca, è riuscito a trovare un modo per bloccare un'intera patch... con un solo segno. So che sembra assurdo, se non impossibile, invece è stato possibile e lui ce l'ha fatta.

La vulnerabilità originale consente ad un criminale non autorizzato di inviare da Outlook un'e-mail contenente un invito con un suono di notifica personalizzato. Questo suono funge da percorso di attacco per stabilire una connessione al server del criminale, fornendo le credenziali NTLM. Da qui, il criminale può utilizzare un attacco di forza bruta per sottrarre le credenziali o eseguire un attacco di inoltro. Tutto ciò può portare, ovviamente, ad un'escalation di privilegi e tutti sappiamo cosa può succedere dopo. La parte peggiore di tutto ciò è che questa vulnerabilità non richiede alcuna azione da parte dell'utente per eseguire l'attacco: una tecnica che rende l'attacco non solo potente ma pericoloso, specialmente se si pensa che l'attacco è partito dalla Russia ed è stato sfruttato in rete, penetrando in varie agenzie governative europee.

La patch è stata pubblicata a marzo ed elimina la possibilità di utilizzare il parametro *PidLidReminderFileParameter,* che consente ai criminali di specificare un percorso personalizzato per dirigere la connessione verso il server dannoso. Utilizzando la funzione *MapURLtoZone*, la patch può controllare se il percorso si sta connettendo a internet. In caso di connessione, viene emesso il suono di notifica, eliminando la possibilità di inserire un percorso per la notifica personalizzata. In teoria, questa procedura dovrebbe impedire a un hacker di sfruttare la vulnerabilità, che dovrebbe eventualmente ricorrere a Internet per stabilire una connessione tra il criminale e la vittima.

> “Gli addetti alla sicurezza hanno così tanto da fare ogni giorno senza doversi preoccupare di nuove vulnerabilità con escalation dei privilegi che non richiedono azioni da parte dell'utente.
>
> **- Tricia Howard, Senior Technical Writer, Akamai**

La lotta alla patch

Qui la cosa diventa interessante e, se posso dire, divertente. Come altri ricercatori di rilievo, Ben ha voluto verificare che la vulnerabilità non fosse effettivamente più sfruttabile. Anche se è un modo troppo semplicistico per porre la questione, ci sono essenzialmente due possibilità per la funzione *MapURLtoZone*: consentire o negare la richiesta. La funzione ricorre a Internet o no? Perlopiù, la patch funziona nel modo previsto: anche se il percorso sembra locale, la funzione *MapURLtoZone* riconosce che il percorso ha intenzione di raggiungere Internet, quindi impedisce di stabilire la connessione.

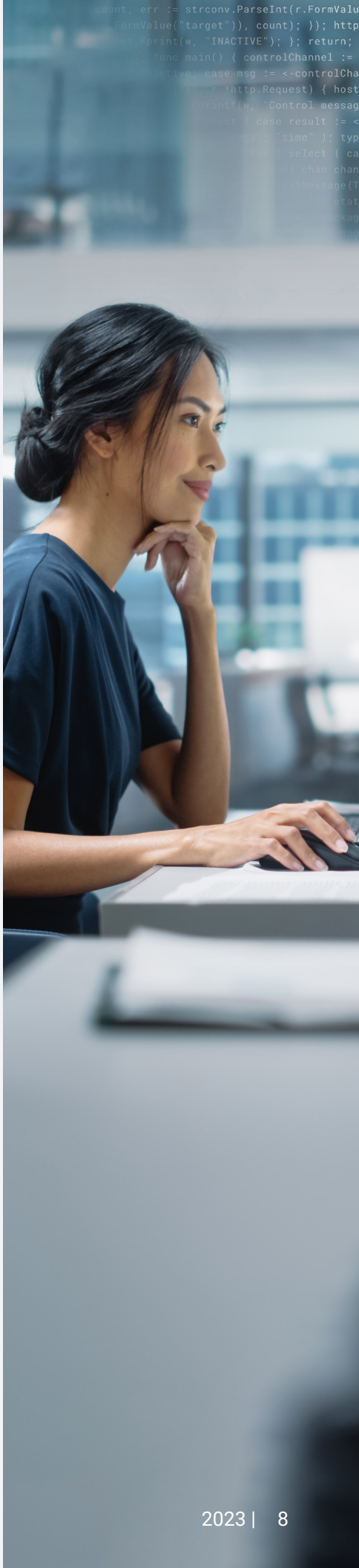
Ben ha deciso di manipolare un po' il nome del percorso aggiungendo il segno "/" alla fine. Se veniva richiesto qualcosa di imprevisto, la funzione *MapURLtoZone* doveva comunque decidere se consentire o negare la richiesta. La barra addizionale non veniva riconosciuta e, pertanto, restituiva uno 0, che la funzione leggeva come locale e considerava affidabile. Quindi, il resto della vulnerabilità era in grado di operare secondo il modo in cui era stata concepita sfruttando *CreateFile* per il percorso personalizzato.

Tutto qui! L'aggiunta di una piccola barra ha reso improvvisamente un'intera patch progettata per una vulnerabilità **critica** una soluzione non più efficace. Questa patch, probabilmente, era stata creata in vari giorni, forse settimane o mesi di lavoro, richiedendo agli esperti di cybersicurezza il tempo e l'energia necessari per eliminare questa minaccia... tutto bloccato da una minuscola barra.

La sofisticazione dell'attacco originale emerge in modo piuttosto sconvolgente quando viene bloccato. In questa fase, il criminale si comporta come Magnus Carlsen con le sue partite di lunga durata. Considerando che una sola barra è riuscita a neutralizzare la patch, è logico pensare che anche il criminale prima o poi sarebbe arrivato ad escogitare un modo per bypassarla. È davvero straordinario il fatto che, invece, Ben abbia scoperto tutto pensando fuori dagli schemi.

Ecco perché i ricercatori che individuano queste vulnerabilità rappresentano davvero la linfa vitale per la comunità degli addetti alla sicurezza Gli addetti alla sicurezza hanno così tanto da fare ogni giorno senza doversi preoccupare di nuove vulnerabilità con escalation dei privilegi che non richiedono azioni da parte dell'utente. I ricercatori della sicurezza fanno davvero la differenza nel mondo, specialmente nel momento in cui diventiamo sempre più dipendenti dalla tecnologia e da Internet nella nostra vita di tutti i giorni.

Sono davvero orgogliosa di far parte di questo team straordinario e di lavorare con alcune delle menti più brillanti su questo pianeta. A chiunque abbia letto i nostri blog, i nostri tweet o i nostri rapporti SOTI, desidero solo dire: Grazie. E ai ricercatori, all'interno e all'esterno del team Akamai SIG, desidero solo dire: Grazie per tutto ciò che fate, bloccate e individuate. Vediamo cosa ci riserverà il prossimo anno, che ne dite?



Minacce ai dati nuove ed emergenti: allerta sugli attacchi Magecart

Sono Chelsea Tuttle e lavoro in Akamai da quasi otto anni. Nel mio ruolo di analista di dati, sono responsabile dei dati presentati nei rapporti SOTI da oltre quattro anni, pertanto trascorro la maggior parte del mio tempo a pulire, esplorare, analizzare e visualizzare i nostri dati. Quando non lavoro sui dati, collaboro strettamente con i redattori dei rapporti SOTI per aiutarli a comunicare le storie che ci raccontano i nostri dati. A causa delle complessità dei big data e dei vantaggi derivanti dalla generazione di rapporti sulla base dei dati cronologici, spesso non aggiungiamo un nuovo dataset, tuttavia, quest'anno l'abbiamo fatto! Ripensando al 2023, le storie da noi pubblicate su questo nuovo database mi ritornano alla mente come tra le mie storie preferite perché mi piaceva il fatto di avere tante opportunità di apprendere nell'ambito di questa impresa.

Troppo spesso nel nostro mondo pensiamo soltanto a segnalare il numero di tentativi di attacco registrati sulla nostra rete e così perdiamo l'opportunità di segnalare i dati rilevanti per la protezione di potenziali vulnerabilità e la prevenzione degli attacchi. Un dataset da noi aggiunto ai nostri rapporti SOTI quest'anno si è particolarmente distinto perché consente di evidenziare in modo esclusivo una potenziale vulnerabilità invece di focalizzarsi sul volume degli attacchi. Questo dataset deriva dalle osservazioni fornite dalla soluzione Akamai Client-Side Protection & Compliance attraverso la sua accurata visione di miliardi di script delle pagine web su base quotidiana. Una delle aree di potenziale vulnerabilità da tenere sotto controllo riguarda il numero di script proprietari e di terze parti che vengono utilizzati nei siti web. Anche se l'utilizzo di uno script proprietario non è sinonimo di sicurezza e l'utilizzo di uno script di terze parti non è sinonimo di vulnerabilità, il maggior livello di fiducia riposto in qualcun altro, come una terza parte che ospita lo script di una pagina web, implica l'aumento dei rischi per un sistema di sicurezza. Akamai sta cercando di colmare il divario esistente tra praticità e sicurezza, che è stato creato dal crescente utilizzo di script di terze parti in tutti i settori.

> “Akamai sta cercando di colmare il divario esistente tra praticità e sicurezza, che è stato creato dal crescente utilizzo di script di terze parti in tutti i settori.
>
> **- Chelsea Tuttle, Senior Data Scientist, Akamai**

Come riportato nel nostro rapporto SOTI Analisi delle tendenze sulle minacce nel settore del commercio, pubblicato a giugno 2023, una delle aree da cui si è focalizzata la ricerca di Akamai quest'anno è stata rappresentata dai recenti attacchi di web skimming di tipo Magecart con una particolare attenzione al modo con cui questi attacchi stanno continuando ad invadere il settore del commercio digitale. Questo tipo di attacco tenta di rubare le credenziali sensibili degli utenti, come i dati delle carte di credito, dal carrello degli acquisti di un sito web di commercio digitale iniettando codice JavaScript dannoso. Questo tipo di attacco tende a risultare semplice per i criminali, tuttavia pone enormi rischi per i consumatori e diventa

sempre più difficile da rilevare. Questi attacchi di web skimming o Magecart spesso si verificano senza che il proprietario o l'utente del sito web se ne rendano conto e i criminali, di solito, scelgono siti web di commercio digitale che utilizzano software obsoleto o vulnerabile.

Le recenti varianti Magecart

Una serie di varianti Magecart si può trovare nelle campagne Magecart più recenti che sono state esaminate dai ricercatori di Akamai. Nel nostro rapporto SOTI di giugno 2023, ci siamo focalizzati sugli attacchi Magecart lato client e abbiamo individuato, negli script di terze parti provenienti dalle librerie open source, alcune vulnerabilità sfruttate, che potrebbero condurre ad attacchi alla supply chain. Subito dopo la stesura del rapporto SOTI, abbiamo pubblicato un blog sul modo con cui i ricercatori di Akamai hanno scoperto una nuova campagna di attacchi Magecart, che sta abusando di siti web legittimi per attaccare altri siti web. In questa campagna, sono stati presi di mira essenzialmente due gruppi di siti web: i siti legittimi, che vengono sfruttati per scopi di hosting e fungono da server controllati dai criminali, e i siti di commercio vulnerabili, che vengono presi di mira da attacchi di web skimming lato client. Un secondo blog pubblicato ad agosto ha descritto come i ricercatori di Akamai hanno scoperto un'altra nuova campagna Magento con un modello SSTI (Server-Side Template Injection) nascosto per estrapolare i dati di pagamento delle vittime dai siti di commercio digitale.

I ricercatori di Akamai hanno scoperto una nuova campagna di attacchi Magecart, che sta abusando di siti web legittimi per attaccare altri siti web

Nell'ultimo blog sugli attacchi Magecart stilato dal team Akamai SIG, viene descritta una nuova tecnica di occultamento, in cui i criminali riescono a manipolare la pagina di errore 404 predefinita di un sito web per nascondere codice dannoso. I ricercatori di Akamai hanno scoperto che questa nuova campagna è costituita da altre due avanzate tecniche di occultamento e mostrano le sofisticate tattiche utilizzate dai criminali per prolungare la catena degli attacchi ed evitare il rilevamento.

Avvicinandoci alla fine del 2023, se ripercorro tutte le opportunità di fare ricerca e di stilare rapporti che abbiamo avuto grazie alle minacce nuove ed emergenti, non posso non attendere con entusiasmo le nuove opportunità legate ai dati e all'apprendimento che ci riserverà il 2024.

Le principali tendenze negli attacchi locali

Mi chiamo Charlotte Pelliccia e sono stata aggiunta al team SOTI nel 2023 per portare alla luce interessanti storie dell'area Asia-Pacifico e Giappone (APJ) e dell'area EMEA (Europa, Medio Oriente e Africa). Le nostre panoramiche sull'area APJ e sull'area EMEA vanno a integrare i nostri rapporti SOTI globali. In questa sede, mi occuperò di riesaminare alcune delle principali tendenze negli attacchi di cui abbiamo parlato nel 2023, aggiornando i dati ricavati dalle nostre panoramiche pubblicate nei primi mesi di quest'anno.

Gli attacchi alle applicazioni web e alle API: racconto di due settori verticali

Coerentemente con i nostri più recenti rapporti SOTI sui servizi finanziari e sul commercio, i servizi finanziari sono rimasti il primo settore verticale per numero di attacchi alle applicazioni web e alle API nell'area APJ, seguiti dal settore del commercio. Dal nostro rapporto pubblicato a giugno 2023, il numero di attacchi contro i servizi finanziari ha raggiunto quota 4,5 miliardi (passando da 3,7 miliardi, con un incremento del 22%). Inoltre, dal nostro rapporto pubblicato a marzo 2023, il numero di attacchi contro il settore del commercio è balzato da 1,2 miliardo a 1,9 miliardi con un incremento del 58%. Le suddivisioni tra i segmenti di mercato secondari rimangono relativamente coerenti (Figura 2).

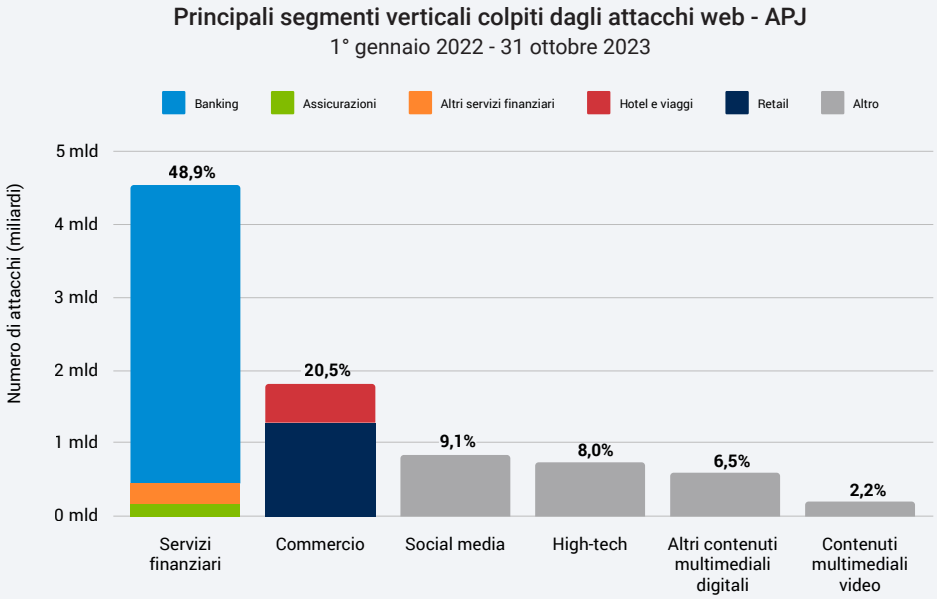


Figura 2. Settori verticali colpiti dagli attacchi web nell'area APJ fino a ottobre 2023

> La visibilità sulle tendenze degli attacchi locali è vitale per aiutare le organizzazioni a comprendere meglio i propri rischi e ad ottimizzare le best practice e gli strumenti utilizzati.
>
> **- Charlotte Pelliccia, Cybersecurity Writer, Akamai**

Contemporaneamente, nell'area EMEA, il commercio rimane il principale settore verticale per gli attacchi alle applicazioni web e alle API, che hanno ora raggiunto una cifra di 6,5 miliardi (passando dai precedenti 4,6 miliardi con un aumento del 41%) a partire dal nostro rapporto di marzo 2023. Anche se il settore manifatturiero è salito al 3° posto dalla quarta posizione per sostituire i servizi finanziari, gli attacchi contro i servizi finanziari sono aumentati del 70% dal nostro rapporto pubblicato a giugno 2023, passando da 1 miliardo a quota 1,7 miliardi. Anche qui, le suddivisioni tra i segmenti di mercato secondari sono rimaste relativamente coerenti (Figura 3).

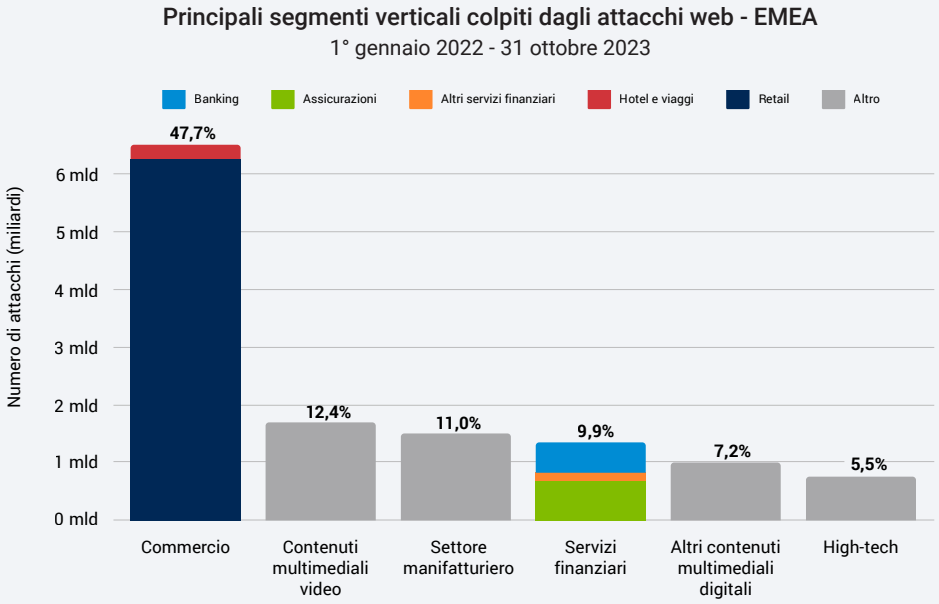
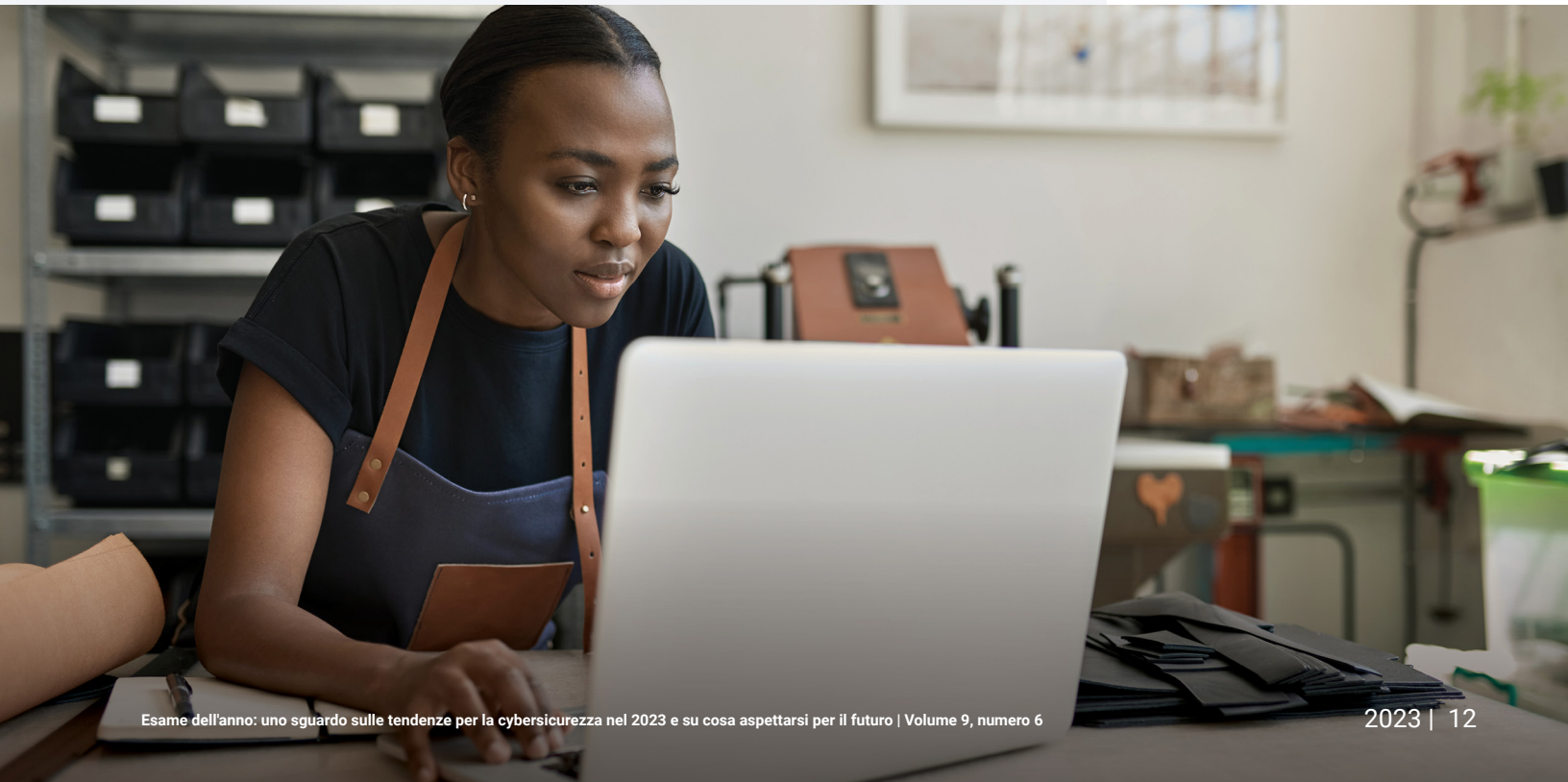


Figura 3. Settori verticali colpiti dagli attacchi web nell'area EMEA fino a ottobre 2023



I bot dannosi sono l'arma preferita dai criminali

Continuando ciò che abbiamo osservato nei nostri precedenti rapporti, l'area APJ è seconda rispetto al Nord America per l'attività di bot dannosi. I primi tre settori verticali colpiti dagli attacchi da gennaio 2022 ad ottobre 2023 nell'area APJ sono il commercio (27,4%), i media video (15,0%) e i servizi finanziari (14,3%). Nell'area EMEA, la metà (50,1%) dell'attività di tutti i bot dannosi ha preso di mira il settore del commercio, seguito dagli altri media digitali con il 15,3% e dai media video con il 12,2% (Figura 4).

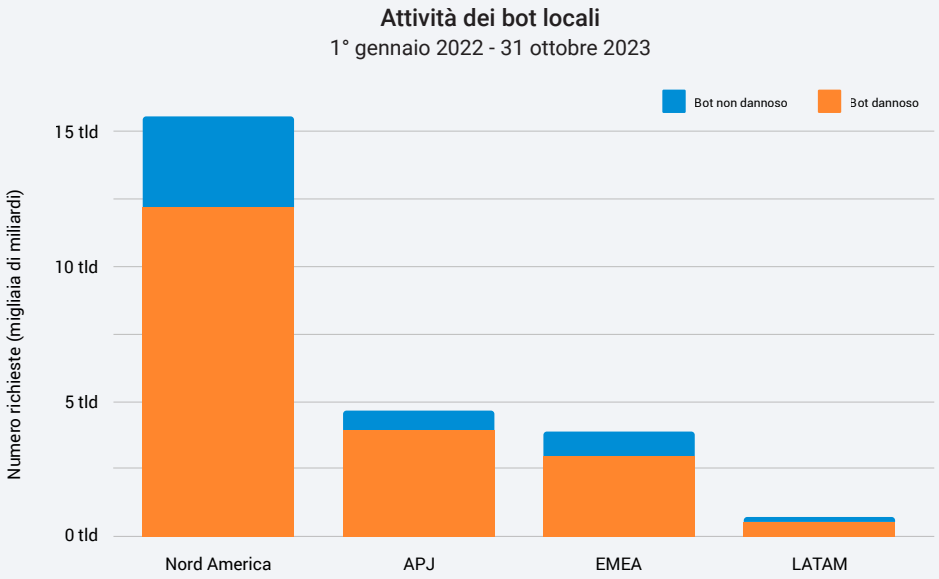


Figura 4. L'utilizzo dei bot dannosi è prevalente in tutte le aree geografiche, superando di gran lunga quello dei bot legittimi

Consultate quanto segue per informazioni fornite dal nostro SOCC sull'evoluzione degli attacchi DDoS e bot.

L'EMEA nel mirino della svolta locale negli attacchi DDoS

Il nostro rapporto del 2023 ha chiarito perfettamente come i criminali abbiano preso di mira proprio l'area EMEA, in parte a causa dell'attuale situazione geopolitica. Un ottimo esempio Il numero degli attacchi DDoS (Distributed Denial-of-Service) contro i servizi finanziari, il settore del gioco d'azzardo e il settore manifatturiero nell'area EMEA ha superato quello di tutte le altre aree geografiche messe insieme (Figura 5).

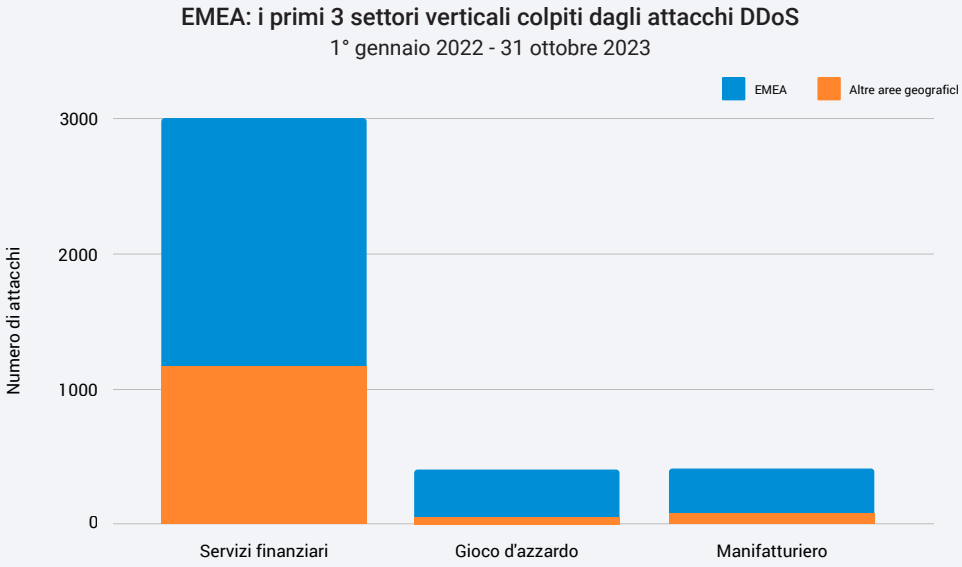


Figura 5. L'EMEA ha subito un maggior numero di attacchi DDoS in questi settori verticali rispetto a tutte le altre aree geografiche messe insieme

Uno sguardo al futuro

Finché i criminali riusciranno a colpire le loro vittime tramite attacchi DDoS, bot e web, è ragionevole aspettarsi che questi metodi rimarranno le loro armi preferite. In realtà, questi tre vettori di attacco si stanno già evolvendo per mantenere o aumentare la loro potenza. Lo sfruttamento delle vulnerabilità zero-day presenti nelle applicazioni web si intreccia con alcune tecniche ransomware (utilizzate da gruppi di ransomware, come CL0P) e include gli attacchi DDoS per creare tattiche di tripla estorsione. Il web scalping tramite i bot è diventato la nuova normalità praticamente per la vendita di biglietti o eventi di quasi tutte le compagnie aeree. Inoltre, stanno aumentando gli attacchi indirizzati alla logica aziendale delle API.

Analogamente, continuano ad aumentare gli obblighi di segnalazione e controllo in base alle normative vigenti in tutto il mondo e per tutti i settori, poiché nessun settore o area geografica si può ritenere al sicuro dagli attacchi. Lo scopo è tenere la legislazione in materia di cybersicurezza aggiornata con il panorama di minacce in costante evoluzione. Le organizzazioni devono rimanere all'erta per soddisfare i requisiti di segnalazione previsti e per tenersi pronte a mitigare i rischi tramite un sistema di difesa multilivello.

Panoramica dalla nostra finestra sul mondo: le informazioni fornite dai nostri SOCC (Security Operations Command Center)

Mi chiamo Roger Barranco e svolgo il ruolo di vicepresidente del reparto Global Security Operations di Akamai, in cui lavoro da quasi 12 anni. Sono responsabile delle operazioni di sicurezza gestite dell'azienda, che si avvale di sei SOCC posizionati in varie sedi nel mondo ed è supportata da un fantastico team. Ho iniziato la mia carriera nel settore della cybersicurezza, che mi ha attirato perché si tratta di un mercato interessante e in continua evoluzione, di cui abbiamo visto un ottimo esempio nel 2023.

Il SOCC di Akamai non è mai stato così oberato di lavoro: entro la fine del 2023, avremo gestito circa il 30% di ticket correlati alla sicurezza in più rispetto allo scorso anno. Ecco alcune delle informazioni chiave che abbiamo ricavato lavorando con i clienti dei nostri servizi di sicurezza gestiti e che le organizzazioni dovrebbero considerare per il 2024.

Il nuovo volto degli attacchi DDoS

Anche se il numero dei clienti presi di mira dagli attacchi storicamente aumenta di anno in anno, oggi il "come" aumenta è cambiato. In primo luogo, il tipo e il volume delle proprietà dei clienti presi di mira sono cambiati. Ad esempio, invece di 10 attacchi sferrati contro endpoint uguali o simili, ora possiamo osservare 100 attacchi tutti diretti contro diversi IP nelle reti dei clienti. Questi attacchi, inoltre, non prendono di mira solo il livello 3, ma anche contemporaneamente il livello 7. Anche gli attacchi contro il DNS sono aumentati notevolmente e perlopiù si tratta di attacchi basati su query in grado di sovraccaricare facilmente l'infrastruttura DNS dei clienti. Solo pochi megabit di traffico DNS indesiderato possono causare un notevole carico di lavoro che grava su un'azienda. Iniziamo anche a vedere un preoccupante aumento dell'attività sul fronte Mirai, che ha guadagnato notorietà per aver sfruttato la potenza dell'IoT (Internet of Things) in modo da causare interruzioni su larga scala.

Nell'odierno scenario delle minacce, non è sufficiente correre ai ripari all'ultimo momento per tenersi al passo con gli attacchi. Le organizzazioni hanno bisogno di un solido servizio di sicurezza nel cloud per gestire questo carico di lavoro mantenendo la loro situazione e implementando, nel contempo, sistemi di protezione esclusivi per ciascuno di questi endpoint. Ecco l'area in cui Akamai eccelle sia da un punto di vista della piattaforma che dei servizi offerti. Possiamo applicare più livelli di sicurezza per difendersi da tutti gli attacchi informatici. Inoltre, i nostri esperti adottano un approccio pratico per esaminare le sfumature e le tendenze di ogni clienti in modo da offrire un monitoraggio e una mitigazione degli attacchi molto specifici in grado di bloccare le minacce e consentire l'ingresso del traffico pulito e previsto.

> “Il SOCC di Akamai non è mai stato così oberato di lavoro: entro la fine del 2023, avremo gestito circa il 30% di ticket correlati alla sicurezza in più rispetto allo scorso anno.
>
> **- Roger Barranco, vicepresidente del reparto Global Security Operations, Akamai**

Lotta contro i bot senza esclusione di colpi

L'abuso di credenziali è difficile da mitigare perché distinguere tra il traffico desiderato e quello indesiderato è complesso e i clienti dispongono di back-end esclusivi che possono richiedere operazioni di mitigazione molto diverse tra loro. Inoltre, i criminali che eseguono attacchi di abuso di credenziali sono tra i più competenti e i più vigili perché un attacco di questo tipo ben riuscito è il modo più semplice per ricavare profitti. Per loro natura pericolosi e costosi, questi attacchi bot rendono importante disporre di una soluzione per la prevenzione degli attacchi di abuso di credenziali, specialmente nei servizi finanziari e nel settore del commercio, in cui continua a crescere l'utilizzo di bot dannosi.

L'EMEA rimane l'area più colpita dagli attacchi

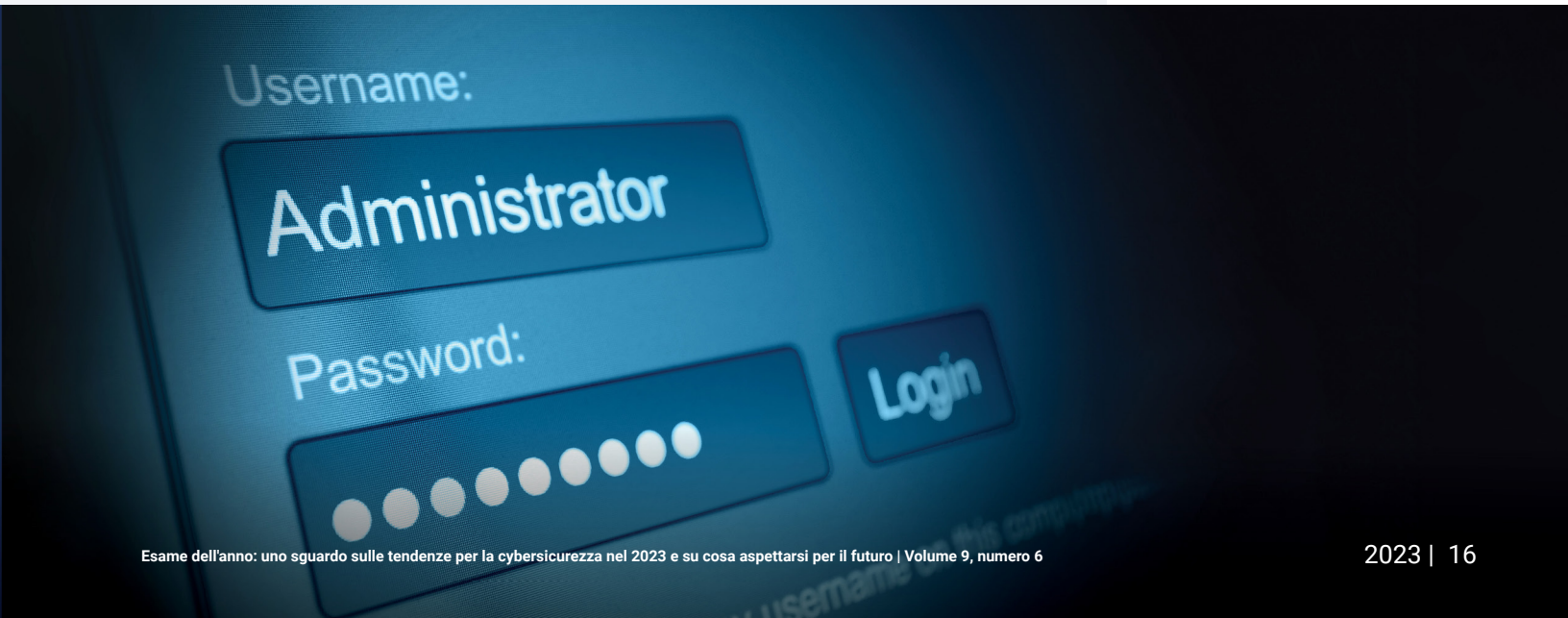
A partire dall'invasione dell'Ucraina, l'EMEA (e l'Europa in particolare) ha rimpiazzato gli Stati Uniti come prima area geografica per numero di attacchi informatici sferrati in diversi settori verticali e sotto forma di varie categorie di tipi di attacco, perlopiù attacchi DDoS. Questa svolta evidenzia il fatto che molti criminali sono sostenuti dai governi o sono simpatizzanti governativi e che il loro interesse sull'Europa non sembra destinato a ridursi.

Criminali sempre più sofisticati

Sono passati i giorni in cui gli script kiddie hanno rappresentato la principale minaccia sfruttando strumenti generici per sferrare un attacco nella speranza di avere fortuna o noleggiando una botnet DDoS per 10 dollari all'ora nell'intento di battere l'avversario di un videogame. Oggi, i criminali sono più sofisticati e sembrano focalizzarsi su specifici obiettivi in dettaglio, pianificando la loro strategia, conducendo operazioni di ricognizione anche con un anno in anticipo e sferrando attacchi per trarre vantaggio di potenziali vulnerabilità. In conseguenza del lavoro preliminare condotto dai criminali, oggi gli attacchi durano di più rispetto agli anni scorsi, quando, di solito, duravano solo pochi minuti.

In conseguenza del lavoro preliminare condotto dai criminali, oggi gli attacchi durano di più rispetto agli anni scorsi, quando, di solito, duravano solo pochi minuti.

- Roger Barranco, vicepresidente del reparto Global Security Operations, Akamai



Best practice per l'allineamento di operazioni e cybersicurezza

Nonostante queste difficoltà, i clienti possono migliorare l'efficacia delle loro azioni per proteggersi dagli attacchi seguendo due best practice per l'allineamento di operazioni e cybersicurezza in modo da consentire ad Akamai di lavorare come un'estensione del proprio team addetto alla cybersicurezza. In primo luogo, i clienti devono collaborare con il SOCC nei periodi più calmi per costruire in modo proattivo un proprio sistema di difesa invece di tentare di farlo durante un attacco. In tal modo, è possibile mitigare tempestivamente gli attacchi senza influire sulla produzione e inviare ai clienti un rapporto di follow-up contenente i dettagli dell'attacco evitato.

In secondo luogo, i clienti devono lavorare in modo proattivo sulla loro prontezza di risposta agli attacchi e su appropriati piani di backup, ad esempio, assicurandosi di sapere come attivare e disattivare il routing di varie piattaforme durante i test. Un attacco di cinque minuti può causare problemi operativi ad un cliente per un'ora, pertanto tenersi pronti per rispondere ad un attacco è importante tanto quanto prepararsi a rispondere ad un problema informatico.

Quest'anno ha messo in evidenza come la cybersicurezza sia in continua evoluzione e questa tendenza è destinata a continuare. La buona notizia è che, applicando queste informazioni, i clienti potranno tenersi al passo con i tempi e proteggersi nel 2024.

I risultati eclatanti illustrati dal nostro Advisory CISO

Mi chiamo Steve Winterfeld e svolgo il ruolo di Advisory CISO in Akamai. In precedenza, ho ricoperto il ruolo di CISO per la Nordstrom Bank e sono stato Director of Incident Response & Threat Intelligence in Charles Schwab. Nell'ambito del mio ruolo, devo garantire che i nostri partner siano in grado di difendere con successo i propri clienti e individuare le aree in cui concentrare le nostre capacità.

Nel corso di quest'anno, ho notato alcune tendenze che mi hanno sorpreso e altre tendenze confermate dai dati da poter utilizzare per aggiornare la nostra strategia. Le mie principali nove storie di quest'anno hanno incluso alcuni risultati eclatanti, alcune notizie attese e alcune cose che sembrano non cambiare mai.

I risultati eclatanti

- Tra il 10% e il 16% delle organizzazioni in totale hanno registrato un traffico di tipo C2 (Command and Control) nelle loro reti almeno una volta ogni tre mesi. Inoltre, il 26% dei dispositivi infetti ha raggiunto domini correlati a un IAB (Initial Access Broker).
- Per quanto riguarda lo scenario delle minacce ransomware, si è notata una preoccupante svolta nelle tecniche degli attacchi con un crescente abuso delle vulnerabilità zero-day e one-day osservato nell'ultimo semestre.
- Dalla ricerca di Akamai, è emerso come le vittime di più gruppi di ransomware hanno quasi 6 probabilità in più di subire un altro attacco nei tre mesi successivi all'attacco iniziale.

Notizie attese

- Gli attacchi indirizzati alla logica aziendale delle API sono complessi da individuare e da mitigare. Di conseguenza, sono difficili da determinare su richiesta individuale.
- Le organizzazioni devono garantire la loro conformità ai nuovi requisiti del PCI DSS (Payment Card Industry Data Security Standard) v4.0 e al regolamento DORA (Digital Operational Resilience Act).

> Le informazioni fornite sono preziose per aiutarvi a pianificare il vostro programma di sicurezza e vedere le aree in cui sono presenti lacune o strumenti ridondanti.
>
> **- Steve Winterfeld, Advisory CISO, Akamai**

Le cose che sembrano non cambiare mai

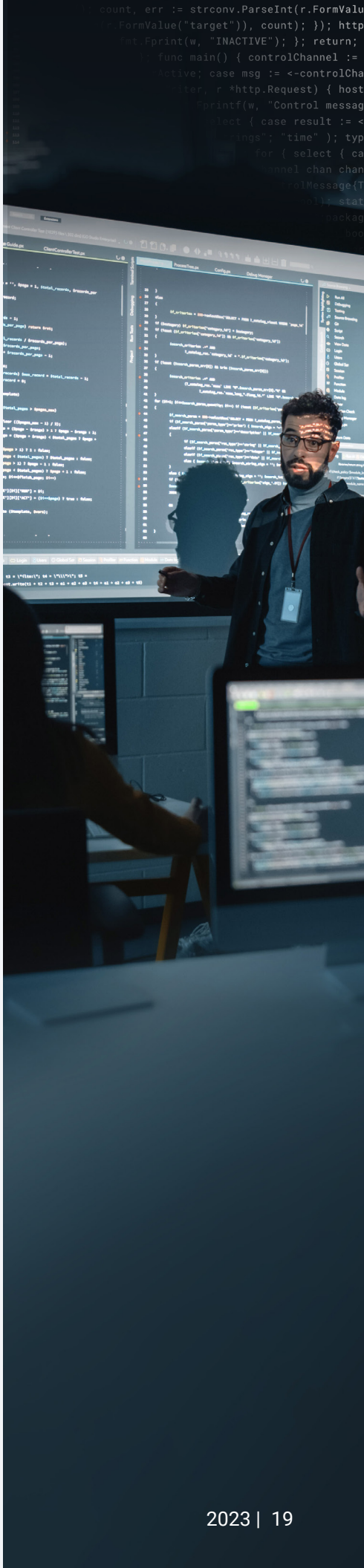
- Il numero di attacchi bot e alle API continua a crescere e, in base ai nuovi dati, soprattutto il numero di attacchi DDoS.
- I settori più colpiti dagli attacchi sono i servizi finanziari, l'high-tech e il commercio.
- L'LFI (Local File Inclusion) è la tecnica di attacco più sfruttata.
- Attualmente, si osserva un cambiamento nell'area geografica in cui si registra il maggior numero di attacchi DDoS, che passa dal Nord America all'Europa.

Una scoperta fondamentale che mi ha fatto pensare è stata rappresentata dagli indicatori di compromissione (IoC) nelle comunicazioni C2. Un aspetto particolarmente destabilizzante è stato costituito dall'alta frequenza del primo rilevamento dopo la violazione dei sistemi da parte di malware, che aveva stabilito una comunicazione. Questo aspetto enfatizza l'equilibrio cruciale che bisogna realizzare tra misure preventive e un rapido rilevamento per minimizzare l'impatto di un attacco.

La storia che mi ha sorpreso di più è stata rappresentata dal passaggio da attacchi contro le persone tramite il social engineering all'utilizzo di attacchi zero-day. Negli ultimi anni, mi è sembrato che le nostre difese tecniche diventassero più solide e ho sentito la necessità di rafforzare il personale con corsi di formazione e sessioni di monitoraggio. Tuttavia, dopo il passaggio di quest'anno agli attacchi zero-day, ho bisogno di esaminare attentamente le aree in cui implementare le risorse per il prossimo anno.

Gli attacchi che sembrano i più dannosi sono quelli che colpiscono un'organizzazione mentre sta subendo o si sta riprendendo da un attacco ransomware.
È semplice focalizzarsi troppo su un momento di crisi e togliere le risorse da un'operazione di monitoraggio dei sistemi di difesa in corso. Questa ricerca è stata concepita con l'intento di ricordare in modo deciso che NON ci si può permettere di abbassare la guardia!

Le informazioni fornite sono preziose per aiutarvi a pianificare il vostro programma di sicurezza e vedere le aree in cui sono presenti lacune o strumenti ridondanti. Potete utilizzare esercizi per aggiornare i vostri playbook/processi, avviare corsi di formazione, ottimizzare i piani per i test di penetrazione o supportare le recensioni sulle soluzioni per la gestione dei rischi. La cybersicurezza è un lavoro di squadra, pertanto queste informazioni possono risultare utili anche per favorire discussioni con i partner interni (come il reparto legale o il team IT) e con i vendor. Come sempre, l'utilizzo di riferimenti/strumenti come il NIST (National Institute of Standards and Technology), la knowledge base di MITRE ATT&CK e l'elenco OWASP con le 10 principali vulnerabilità per la sicurezza delle API si rivela una preziosa risorsa.



Uno sguardo al futuro

Predire il futuro è impossibile, ma possiamo anticipare che gli attacchi DDoS e alle API domineranno nel 2024. I continui sforzi volti a creare armate di botnet più vaste e a sviluppare nuove tecniche, insieme al sostegno dei governi, causeranno un aumento nel numero di attacchi DDoS. Questo fattore, insieme con l'evoluzione del ransomware, sarà la genesi della legislazione e della resilienza.

La trasformazione continua a favorire l'implementazione delle API nella maggior parte dei settori. Questa rapida crescita condurrà inavvertitamente ad un ampliamento delle superfici di attacco e ad un aumento delle vulnerabilità, delle API ombra o API "zombie" e ad un maggior abuso delle API. Prevediamo di registrare una significativa crescita nel numero di attacchi alle applicazioni web e alle API tramite l'utilizzo di vettori di attacco standard, come l'LFI, e di tecniche emergenti, come SSRF (Server-Side Request Forgery) e SSTI (Server-Side Template Injection), che si serviranno di strumenti per rilevare il movimento laterale e per mitigare l'impatto degli attacchi.

Infine, tranne alcune tendenze di settore e locali, prevediamo di registrare una carenza complessiva di esperti di cybersicurezza competenti. L'apprendimento automatico e l'intelligenza artificiale di un modello linguistico di grandi dimensioni potranno risultare utili, tuttavia, nel complesso, risulterà estremamente difficile individuare e mantenere i talenti di cui abbiamo bisogno. Pertanto, verrano instaurate partnership con i vendor per garantire la presenza di personale on-demand o servizi gestiti per le funzioni non essenziali.

Per quanto riguarda il team Akamai SIG, continueremo a mantenere alto il livello di allerta riguardo alle minacce prevalenti e ai rischi alla sicurezza che spuntano all'orizzonte. Ci terremo in contatto con la community della sicurezza tramite le nostre piattaforme e i nostri canali per sostenere l'impegno volto alla costruzione di un'intelligence sulle minacce. Inoltre, nel 2024, festeggeremo il 10° anniversario dei nostri rapporti SOTI! Siamo entusiasti di continuare a migliorare i nostri rapporti con l'introduzione di nuovi dataset, ausili visivi e informazioni preziose per supportare gli addetti alla sicurezza nel perseguire l'obiettivo di mantenere protette le loro organizzazioni.

Saremo lieti di condividere con voi altri risultati emersi dalle nostre ricerche nel corso del prossimo anno. Nel frattempo, state al sicuro!

Riconoscimenti

Editoria e stesura

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

Revisione e contributi di esperti del settore

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Analisi dei dati

Chelsea Tuttle

Marketing ed editoria

Georgina Morales Hampe
Emily Spinks

Altri rapporti sullo stato di Internet - Security

Leggete i numeri precedenti e guardate le prossime uscite degli acclamati rapporti sullo stato di Internet - Security di Akamai sul sito **akamai.com/soti**

Ulteriori informazioni sulla ricerca delle minacce Akamai

Restate aggiornati con le ultime intelligence sulle minacce, rapporti sulla sicurezza e ricerche sulla cybersicurezza. **akamai.com/security-research**

Accesso ai dati del rapporto

Potete visualizzare i grafici e i diagrammi citati in questo rapporto in versioni di alta qualità. L'utilizzo e la consultazione di queste immagini sono forniti a scopo gratuito, purché Akamai venga debitamente citata come fonte e venga conservato il logo dell'azienda: **akamai.com/sotidata**.

Ulteriori informazioni sulle soluzioni Akamai

Per ulteriori informazioni sulle soluzioni Akamai per la protezione dalle minacce, visitate la nostra **pagina sulle soluzioni per la sicurezza**.

Akamai

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn.
Data di pubblicazione: 11/23.