MARKET PERSPECTIVE

# WAF lato client: la nuova frontiera della sicurezza

Christopher Rodriguez

## EXECUTIVE SNAPSHOT

## FIGURA 1

**Executive Snaphot: minacce per i client e soluzioni emergenti**

Nel 2018, i ricercatori nel campo della sicurezza hanno identificato una nuova forma di crimine informatico denominata skimming delle carte di credito online o web skimming. Gli attacchi Magecart hanno sfruttato la crescente tendenza di spostare le funzionalità delle applicazioni dal server al client. I criminali sono riusciti a iniettare un codice dannoso in origini di applicazioni fidate, che veniva eseguito nel browser degli utenti, al di fuori della protezione di un WAF. Alla fine, gli attacchi hanno rappresentato una violazione di dati di lunga durata che ha esposto un anello debole nelle pratiche di sicurezza delle applicazioni web dell'azienda.

### Concetti chiave

- Gli script lato cliente sono uno strumento prezioso nell'architettura di un'applicazione, in quanto offrono i vantaggi di user experience, performance delle applicazioni, analisi e sicurezza ottimizzati.
- Gli script sono ovunque. I siti web di oggi hanno decine di script diversi e 2 su 3 sono script di terze parti.
- Gli script lato client rappresentano un delicato ma dinamico ecosistema di funzionalità, con molte parti interessate.
- Di seguito sono riportate le best practice di base per la sicurezza lato client. Tuttavia, le complessità e le sfide della sicurezza lato client aumenteranno la richiesta di soluzioni per la sicurezza aziendale per questo vettore di attacco.

### Azioni raccomandate

- Le soluzioni disponibili sul mercato variano drasticamente in base alle funzionalità. Per gli acquirenti, il desiderio principale è quello di bilanciare la sicurezza e il requisito aziendale di "non rovinare tutto".
- La visibilità e il controllo lato client non sono un'area molto facile o familiare per molti fornitori. I nuovi operatori di mercato considereranno attentamente se creare da soli le proprie soluzioni o se scegliere funzionalità esistenti da acquisire o integrare.
- Molte organizzazioni IT non dispongono di informazioni dettagliate su script o ambienti lato client. Ancora meno comprendono i problemi di sicurezza. È necessario un elevato livello di conoscenza del mercato inclusi demo, ricerche, modelli di verifica e versioni di prova.

Fonte: IDC, 2021

April 2021, n. IDC US47623221

## NUOVI SVILUPPI E DINAMICHE DI MERCATO

Questo documento di IDC propone un'analisi del vettore di attacco, delle soluzioni emergenti e del futuro del mercato delle soluzioni WAF (Web Application Firewall) lato client.

Akamai, Cymatic, PerimeterX e Tala Security stanno tracciando nuovi percorsi estendendo la protezione WAF per rispondere alle minacce lato client. Gli script lato client rappresentano un vettore di attacco emergente e il mercato di soluzioni di sicurezza sta evolvendo per rispondere a questa necessità.

In generale, queste soluzioni per la sicurezza vengono denominate *anti-scripting, "WAF lato client"* o *sicurezza degli script,* tuttavia la terminologia può generare confusione. Considerate le seguenti opzioni:

- Un WAF evoca alla mente un set specifico di controlli che si applicano alle applicazioni web, sebbene gli script lato client siano un punto di controllo intrinsecamente diverso nel paradigma della sicurezza delle applicazioni.
- WAF lato client è un termine utile per mettere in relazione un controllo di sicurezza comprovato in WAF, mentre il termine "sicurezza degli script" può essere nebuloso e confusionario al confronto.
- L'anti-scripting generalizza gli script come una tecnologia indesiderata, inefficiente o assolutamente dannosa. In realtà, gli script rappresentano uno strumento prezioso e potente per l'architettura delle applicazioni.

Nel complesso, IDC fa riferimento a queste soluzioni principalmente come WAF lato client, per i vantaggi della familiarità associata con il WAF. Inoltre, il termine WAF lato client mantiene la possibilità di un'espansione futura di tipi di minacce sul lato client al di là degli script.

## Introduzione

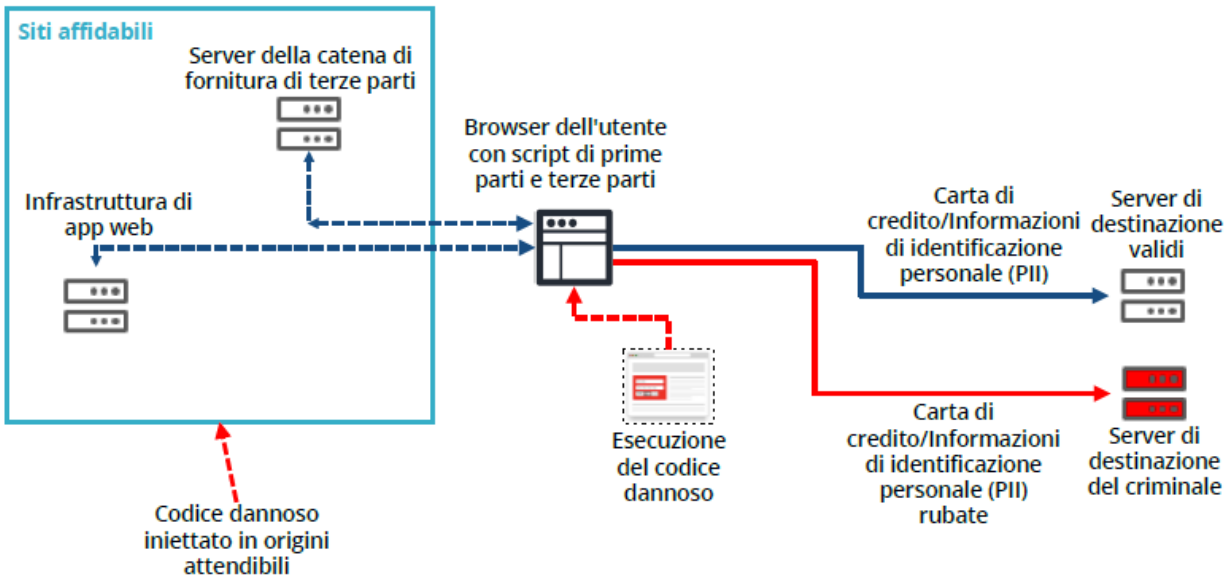
Nel 2018 è emersa una nuova tecnica per rubare i dati delle carte di pagamento, attribuita al gruppo di hacker Magecart. Gli attacchi Magecart hanno sfruttato un nuovo vettore: gli script che vengono eseguiti nei browser client. Una volta individuata la campagna di attacchi, le indagini hanno dimostrato che il gruppo Magecart aveva compromesso per mesi i siti web di grandi aziende online, tra cui Ticketmaster, NewEgg e British Airways.

La campagna Magecart ha usato gli attacchi lato client per eseguire il web skimming (che può essere anche definito come furto di carte online o form jacking). Il web skimming è uno degli aspetti più altamente visibili di questo vettore di attacco, tuttavia questo vettore facilita altri attacchi, come quelli di watering hole e cryptojacking. L'obiettivo di questi attacchi può variare ma, nel complesso, la sicurezza lato client nasconde un potenziale per le campagne di furto di dati che possono sfociare in violazioni dei dati massicce e di lunga durata.

La figura 2 offre una panoramica del ciclo di vita di un attacco lato client. Nota: il codice dannoso viene eseguito nel browser, al di fuori della protezione offerta da una soluzione WAF. Inoltre, il codice dannoso può essere inserito sia su fonti di terze parti sia di prime parti.

## FIGURA 2

### Anatomia di un attacco web skimming (nel browser)




Fonte: Akamai, 2021

## Dinamiche del settore

Il WAF lato client è un mercato nascente con un forte potenziale di crescita. Questa tecnologia interviene su un vettore di attacco emergente, risultato di un cambio nelle pratiche di sviluppo delle applicazioni. Negli ultimi anni, le funzionalità delle applicazioni sono state spostate dai server ai client ed è improbabile che la tendenza rallenti. Il passaggio delle funzionalità dai server ai client scarica le richieste di performance dal server, consentendo performance ed experience interattive migliori per gli utenti finali. Di conseguenza, gli script sono strumenti sempre più popolari per il miglioramento delle esperienze online interattive. Gli script vengono usati per una gamma varia e ampia di scopi legittimi, tra cui monitoraggio, analisi, user experience e sicurezza. Gli script sono onnipresenti nei siti web di oggi, con una media di almeno 15 script a sito, secondo alcune stime.

Inoltre, la semplicità di JavaScript ha spinto l'adozione dello scripting da parte di persone diverse dai professionisti IT. Gli script consentono alle business unit al di fuori dei reparti IT di creare e inserire codice nelle risorse web per vari scopi. Gli script consentono anche un'integrazione e un inserimento più semplice di servizi di terze parti. Tuttavia, l'aspetto della sicurezza degli script resta largamente sottovalutato, specialmente tra le aziende che continuano a concentrarsi su strumenti essenziali come il WAF.

Nel complesso, la minaccia non è compresa pienamente. Le violazioni più ampiamente discusse in questa categoria si incentrano sugli script di terze parti. La campagna Magecart è un esempio pertinente. In quel caso, gli hacker di Magecart accedevano al codice di un partner fornitore dell'azienda presa di mira e inserivano il codice dannoso in script affidabili. Per alcune aziende, la sensazione è che il nuovo vettore di attacco punti a "cambiare le regole del gioco". Già proteggere un sito web contro le tante minacce che le imprese online devono affrontare non è un compito semplice, dover poi tenere conto anche delle vulnerabilità dei sistemi dei partner è davvero troppo. Gli script di

terze parti sono i più problematici in quanto i dipartimenti IT non hanno visibilità o controllo sul codice, sugli aggiornamenti o sulle modifiche dei partner.

Sfortunatamente, il web skimming è solo una parte del problema in quanto gli script di terze parti rappresentano solo un dato demografico degli script presenti nella maggior parte delle pagine web. Per fornire un esempio, si consideri che i ricercatori di Akamai hanno stimato che circa il 67% degli script deriva da terze parti. Fondamentalmente, la maggior parte delle pagine web è un ecosistema di script di parti interessate interne e esterne all'azienda. Questi sistemi interni possono veicolare codici dannosi nel caso in cui i server venissero sabotati.

Esistono alcune best practice che aiutano a ridurre il rischio. Un rigido controllo degli script di terze parti è un punto di partenza intelligente. Anche le revisioni regolari del codice e i test delle applicazioni sono pratiche affidabili. Inoltre, i dipartimenti IT possono sfruttare tecnologie come la Subresource Integrity (SRI) per individuare le modifiche agli script. Sebbene queste opzioni possano fornire una linea base di protezione, la storia ha dimostrato che i criminali impiegano costantemente tattiche avanzate e intelligenti per evitare il rilevamento. Di conseguenza, la SRI e le altre pratiche rappresentano un punto di partenza utile, ma sono limitate contro gli attacchi avanzati.

Inoltre, è improbabile che i criminali rallentino le loro azioni, a meno che non siano obbligati a farlo. Dai primi e famosi attacchi Magecart, gli hacker si sono evoluti di continuo. Ad esempio, gli hacker possono prendere di mira le reti di inserzionisti come mezzo per iniettare il codice dannoso tramite i banner pubblicitari. O ancora possono puntare agli archivi di codice, come GitHub. Questi archivi includono librerie e frammenti di codice open source, che vengono generalmente riutilizzati e considerati attendibili da molte aziende, che li usano a loro volta nelle loro applicazioni web. Di conseguenza, queste fonti attendibili rappresentano un potenziale veicolo per l'inserimento di script dannosi in siti web altrimenti sicuri.

Ogni fornitore approccia il problema in modo leggermente diverso. Le soluzioni disponibili sul mercato vengono ampiamente implementate tramite i tag JavaScript, il che consente di inserire la funzione di sicurezza prima che gli script possano essere eseguiti. Da qui, le soluzioni divergono enormemente. Le funzionalità principali tendono a includere la visibilità e la mappatura di script e comunicazioni (ad esempio, l'origine e la destinazione). Funzionalità aggiuntive includono la gestione delle vulnerabilità, l'applicazione delle policy e il rilevamento di attività dannose ed eventi sospetti. Sono possibili funzionalità più avanzate, come la crittografia di chiavi e dati integrati, l'offuscamento del codice, il sandboxing e altre misure difensive. Per ora, questo approccio sembra offrire una visibilità e un'automazione sufficienti delle funzionalità di sicurezza principali. Mentre si auspica l'avvento di misure di rilevamento più sofisticate nel tempo, l'enfasi continua a concentrarsi sul fornire una sicurezza sufficiente senza interrompere l'experience degli utenti finali o "compromettere" la funzionalità dei siti web.

## Esempi di fornitori

Al momento, sono disponibili poche offerte di WAF lato client, le quali variano per campo d'azione e funzionalità. Esiste una manciata di specialisti del mercato, tra cui Digital.ai (precedentemente noto come Arxan), Source Defense, Cymatic, Tala Security e ChameleonX (acquisito da Akamai nel 2019). Altri propongono varie soluzioni per la sicurezza delle applicazioni web. Ad esempio, nel 2020 Akamai ha introdotto Page Integrity Manager come parte del suo approccio di protezione dagli attacchi multivettore, tramite un portfolio olistico di soluzioni per la sicurezza di applicazioni web e API. Allo stesso modo, PerimeterX ha presentato la sua offerta nel 2019 come complemento alla sua soluzione enterprise per la gestione dei bot. L'operatore più recente è Cloudflare, che ha introdotto la sua nuova soluzione nel marzo 2021. IDC nota che queste aziende vantano un background nella gestione

dei bot che può aver aiutato a fornire un livello di familiarità con la sicurezza lato client. La gestione dei bot è un processo difficile da svolgere bene e le soluzioni migliori tendono ad implementare tecniche multiple (incluso JavaScript) per rilevare e catalogare il comportamento dei bot.

Gli attacchi lato client possono essere difficili da rilevare. Tuttavia, una volta che sono state individuate, queste minacce sono abbastanza chiare in termini di costi finanziari per le aziende interessate e i loro clienti. Ad esempio, queste violazioni dei dati possono essere, spesso, misurate in termini di numero di record di clienti rubati. I concorrenti attuali hanno dimostrato un elevato livello di efficacia nell'individuazione e nella mitigazione delle minacce basate sugli script. Ciò costringe i criminali a concentrare le loro azioni altrove, pertanto il problema continua a presentarsi. Per i criminali, l'obiettivo è quello di trovare siti web non protetti o poco protetti da attaccare. Nonostante la visibilità degli attacchi Magecart, la consapevolezza del mercato riguardo al vettore di attacco resta bassa, il che consente ai criminali di trovare nuovi obiettivi a cui puntare. Probabilmente, tutti questi fattori contribuiranno a sensibilizzare la consapevolezza generale in merito a questo vettore di attacco, il che aumenterà le richieste dell'utenza e attirerà altre aziende verso il settore negli anni a venire.

## Strategie di mercato

Le minacce sul lato client rappresenteranno un problema per le imprese online fin quando i criminali informatici considereranno redditizio questo vettore di attacco. Tuttavia, si tratta di un tipo di attacco decisamente più mirato rispetto agli attacchi sferrati in massa, come i ransomware. Ci vorrà del tempo prima che la maggior parte delle aziende prese di mira riesca a individuare e mitigare gli attacchi basati sugli script. Potrebbero volerci molti sforzi anche per aumentare la consapevolezza generale del mercato in relazione a questi problemi. I fornitori hanno difficoltà a far aumentare la consapevolezza tramite la formazione continua, le dimostrazioni e i test dei modelli di verifica.

Probabilmente, molte aziende introdurranno prodotti e funzionalità per conto proprio. Akamai ha presentato Page Integrity Manager un anno fa per affrontare il problema dell'espansione della superficie di attacco creata dagli script caricati nei browser, dove si inviano e si visualizzano informazioni di identificazione personale (PII). Sempre in questo ambito, le minacce sul lato client hanno proliferato nel 2020, quando l'uso di Internet per le transazioni è aumentato a causa del COVID-19.

Cloudflare è l'aggiunta più recente al mercato, con l'introduzione di una nuova soluzione denominata Cloudflare Page Shield. Prima di ciò, Cloudflare ha affrontato questo vettore di attacco tramite una partnership tecnologica con Tala Security.

Mentre Cloudflare ha deciso di sviluppare le proprie funzionalità per la sicurezza lato client, IDC nota che questo approccio potrebbe non essere così semplice da seguire da parte di altri. Per la maggior parte dei fornitori del mercato, lo sviluppo di funzionalità WAF lato client è stato preceduto da tecniche di gestione dei bot che sfruttano i client JavaScript. Le soluzioni WAF esistenti non dispongono di queste funzionalità o di esperienza con il codice lato client.

Per i fornitori che stanno potenziando le loro linee di prodotti per la sicurezza di applicazioni web e API, l'acquisizione di soluzioni specializzate può rappresentare la migliore opzione per pareggiare le forze in campo. L'acquisizione di ChameleonX da parte di Akamai offre un esempio dei potenziali vantaggi del combinare tecnologie appositamente progettate con il cloud su larga scala. Page Integrity Manager protegge più di 3,7 miliardi di visualizzazioni di pagine al mese, analizzando 6,4 miliardi di esecuzioni di script al giorno. Approssimativamente, ogni settimana vengono osservate 40 milioni di

interazioni di utenti finali sospette e dannose, il che consente ad Akamai di fornire notifiche in tempo reale, analisi delle cause di fondo, mitigazione immediata e creazione di policy di automazione.

## IL PUNTO DI VISTA DI IDC

Gli attacchi lato client saranno una crescente lacuna nella sicurezza fino a quando i criminali informatici considereranno redditizio questo vettore di attacco, il che potrebbe significare molti anni. Una ragione significativa è che il vettore di attacco lato client non è ancora ben compreso. Tradizionalmente, le funzioni WAF lavorano analizzando il traffico delle applicazioni web che arriva al server web. Dal momento che JavaScript è diventato più popolare nel corso degli anni, una significativa quantità di funzionalità è stata migrata sui browser client. Tuttavia, molte aziende sottovalutano queste dinamiche o non hanno esaminato in modo approfondito i rischi e le implicazioni in termini di sicurezza della migrazione delle funzionalità web sui browser client.

Il fatto che questo tipo di attacco sia decisamente più mirato rispetto agli attacchi sferrati su larga scala, come i ransomware, sta contribuendo ulteriormente all'elevato livello di confusione nel mercato. Ad esempio, molte aziende hanno grande familiarità con i tipi di attacchi risolti dal WAF e dalle soluzioni di mitigazione degli attacchi DDoS. Il rischio per la sicurezza rappresentato dai bot indesiderati e dannosi è un'altra pratica che sta guadagnando una diffusa consapevolezza. Tuttavia, aree quali la sicurezza delle API e la sicurezza lato client sono problematiche emergenti che pur non essendo visibili rappresentano un rischio significativo, esattamente come la parte sommersa di un iceberg (vedere la Figura 3).

## FIGURA 3

### L'iceberg della sicurezza delle API e delle applicazioni web


Fonte: IDC, 2021

Una volta che un'azienda ha compreso il potenziale vettore di attacco, il processo di catalogazione e comprensione degli script che vengono eseguiti in un ambiente IT complesso, con diversi domini, pagine web e applicazioni web, rappresenta un'impresa titanica. Al tempo degli attacchi Magecart, il processo di individuazione degli script dannosi inseriti consisteva nella revisione manuale riga per riga del codice, al fine di individuare le modifiche. Adesso, questo processo è stato semplificato, in quanto i ricercatori conoscono i problemi sottostanti e le best practice. Tuttavia, resta il fatto che ci vorrà del tempo prima che la maggior parte delle aziende prese di mira riesca a individuare e mitigare gli attacchi basati sugli script, perché ci vuole tempo innanzi tutto per scoprire il vettore di attacco e poi per identificare eventuali lacune o vulnerabilità di sicurezza esistenti. Inoltre, questo vettore di attacco è un bersaglio mobile, in quanto il 75% degli script viene modificato ogni trimestre. Ogni nuova modifica apre la possibilità di introdurre nuove vulnerabilità e codici dannosi.

Il tempo resta comunque un fattore essenziale. Le violazioni note dovute ad attacchi lato client sono in atto da molto tempo e hanno dato ai criminali mesi di vantaggio. Durante questo periodo, un numero infinito di carte di credito e altre informazioni di identificazione delle persone sono state rubate. Una volta individuato un attacco, gli autori sono liberi di chiudere i battenti e iniziare daccapo con una nuova vittima. Essenzialmente, occorre molto tempo per individuare gli attacchi lato client e questo squilibrio rappresenta un enorme vantaggio per i criminali informatici, che deve essere necessariamente ridotto.

Inoltre, il tempo è il più grande ostacolo per educare il settore della sicurezza e aumentare la consapevolezza degli acquirenti aziendali di tecnologie riguardo al problema. I fornitori hanno difficoltà a far aumentare la consapevolezza tramite la formazione continua, le dimostrazioni e i test dei modelli di verifica. Akamai, ad esempio, sta offrendo una versione di prova gratuita della sua soluzione Page Integrity Manager. Questa soluzione offre una panoramica dell'ecosistema degli script delle pagine web prese di mira, insieme all'analisi dei vari script, delle vulnerabilità e dei fattori di rischio. Anche altri fornitori offrono versioni di prova, dimostrazioni e formazione.

IDC elogia questi approcci. Nulla spiega meglio l'urgenza di una situazione o il valore e l'efficacia di una soluzione di sicurezza di una verifica sul campo. Per i fornitori, il vantaggio di una potenziale conversione ad abbonamenti premium è chiaro. Anche per gli acquirenti il vantaggio è sostanziale, in quanto ottengono la visibilità su un vettore di attacco che è stato tradizionalmente un punto cieco per la maggior parte delle aziende.

Per i prossimi anni, IDC monitorerà il mercato delle soluzioni WAF lato client per comprenderne l'impatto su mercati affermati quali WAF, mitigazione degli attacchi DDoS, gestione dei bot e prevenzione delle frodi online. Una volta risolto il punto cieco della sicurezza lato client, saranno necessarie discussioni più approfondite sull'impatto delle potenziali funzionalità di visibilità e applicazioni client, come un punto di controllo per la sicurezza.

## ULTERIORI INFORMAZIONI

### Ricerche correlate

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, ottobre 2020)
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, settembre 2020)
- *IDC Market Glance: Software-Defined Secure Access, 2Q20* (IDC #US46291520, maggio 2020)
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value* (IDC #US46022619, febbraio 2020)
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms* (IDC #US46075520, febbraio 2020)

### Sinopsi

Questo documento di IDC propone un'analisi del vettore di attacco, delle soluzioni emergenti e del futuro del mercato delle soluzioni WAF lato client. Pochi dipartimenti IT vantano una comprensione completa delle minacce che colpiscono gli script lato client che vengono eseguiti nei loro ambienti web. I criminali informatici hanno preso di mira gli script lato client come mezzo per eseguire furtivamente codice dannoso, al fine di ottenere un enorme guadagno finanziario senza il rischio di essere catturati. Dal momento che questo vettore di attacco crescerà nei prossimi anni, la richiesta di soluzioni WAF lato client aziendali aumenterà costantemente.

"Lo script lato client è la nuova frontiera per la sicurezza. I criminali informatici sono inarrestabili nella loro ricerca di vantaggi economici e hanno individuato una nuova lacuna negli stack di sicurezza digitale delle imprese", afferma Christopher Rodriguez, Research Manager, IDC Network Security Products and Strategies.

## Informazioni su IDC

Fondata nel 1964, IDC (International Data Corporation) è la prima società mondiale specializzata in market intelligence, servizi di advisory e organizzazione di eventi nell'ambito digitale e ICT. Oltre 1.100 analisti a copertura di 110 Paesi del mondo mettono a disposizione a livello globale, regionale e locale la loro esperienza e capacità per assistere il mercato della domanda e dell'offerta nella definizione delle proprie strategie tecnologiche e di business a supporto della competitività e crescita aziendale. Ogni anno, IDC conduce 300.000 interviste, pubblica 5.000 report e ospita 10.000 CIO ai propri eventi.

## Global Headquarters

5 Speen Street
Framingham, MA 01701
Stati Uniti
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

---