citrix

White Paper

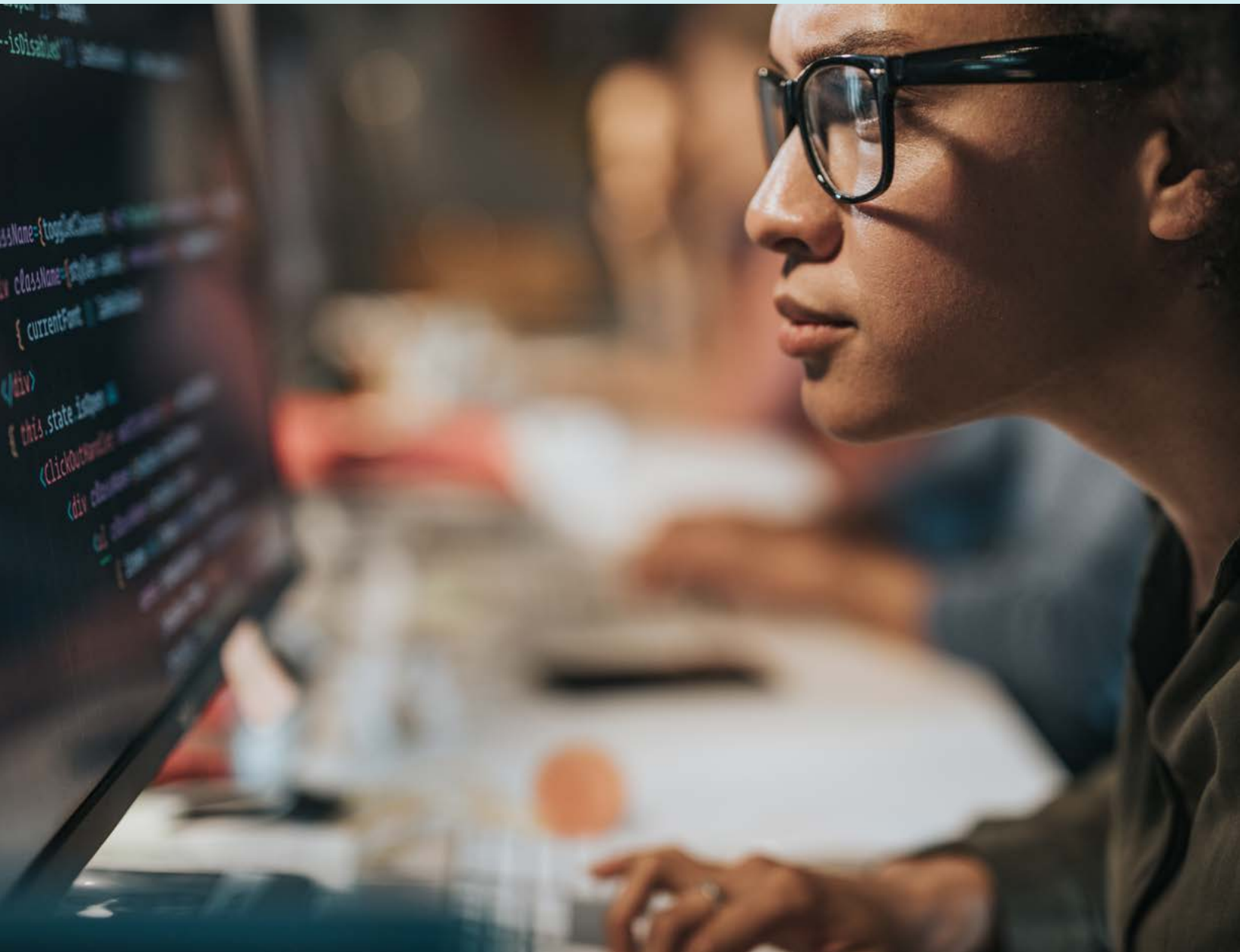
BOT Management

Che cos'è, perché ormai riguarda tutte le imprese e cosa si rischia se non si fa.

Se ti preoccupano le interferenze dei tuoi competitor, se non ti spieghi degli strani incrementi nei costi o non sai come affrontare il rischio DDos, forse alla gestione dei BOT non hai ancora dedicato tutta l'attenzione che serve.

È di pochissimi giorni fa la notizia che i portali di alcune importanti istituzioni italiane sono stati oggetto di una serie di attacchi informatici che ne hanno compromesso, in modo più o meno esteso, la piena funzionalità. È solo l'ultimo episodio di un'ondata pressoché costante di attacchi che colpiscono l'Italia, anche se la situazione è praticamente identica in qualsiasi altro paese del mondo. Chi più, chi meno, tutti subiscono degli attacchi cibernetici. Difatti, nell'arco di circa 20 anni, i termini DoS (Denial of Service) e soprattutto DDoS (Distributed Denial of Service) si sono diffusi ben oltre la ristretta cerchia degli addetti ai lavori, entrando a far parte del lessico comune.

Nel caso più recente, l'elemento di novità rispetto al passato non è quindi nel fatto che dei siti web siano stati messi fuori uso per alcune ore, quanto che in almeno in una delle sue connotazioni, l'attacco abbia avuto caratteristiche particolari: non ha saturato il link, né ha sfruttato particolare vulnerabilità del protocollo HTTP o del front end web, ma ha "semplicemente" portato a saturazione le risorse dei server con una serie di richieste lecite provenienti da decine di migliaia di indirizzi IP. In pratica, usando un'armata di BOT, gli attaccanti hanno fatto in modo che i siti arrivassero al limite della propria capacità utilizzando, ancora una volta, un attacco noto, lo Slow HTTP.

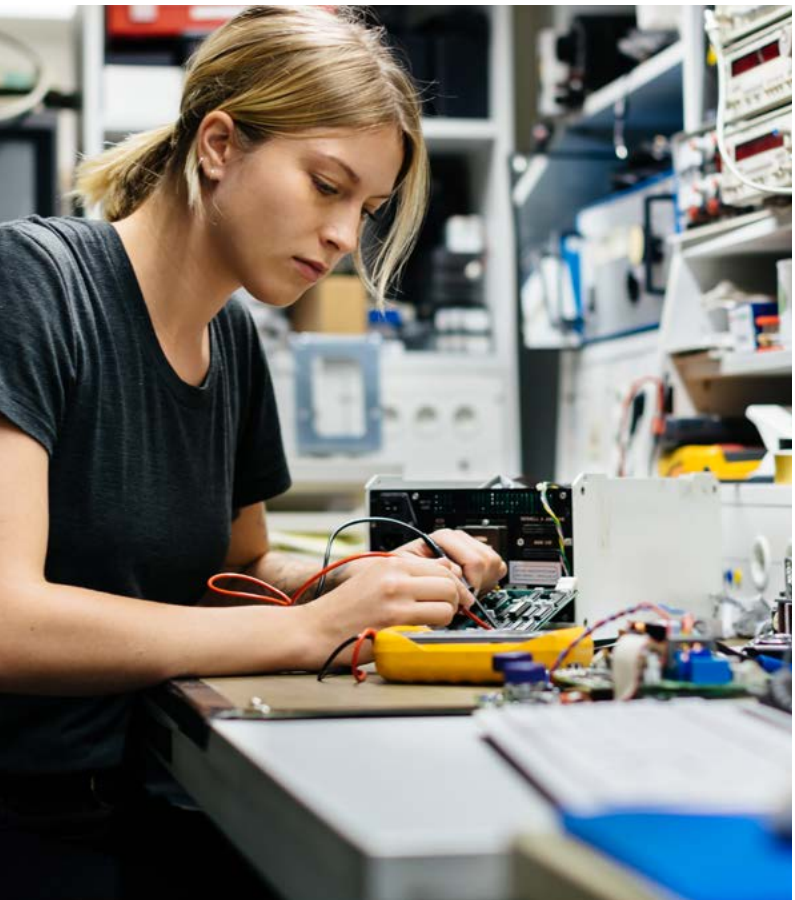


Cosa sono i BOT

Come detto, l'ondata di attacchi ha quindi visto per protagonisti dei BOT, un termine probabilmente meno conosciuto, che deriva da "Robot" e che identifica una famiglia piuttosto vasta di programmi che simulano il comportamento di utenti per eseguire una serie di azioni, normalmente in tempi e con modi che non sono umani.

I BOT rappresentano ormai una presenza molto "ingombrante" sulla rete. Si stima che attualmente, quasi il 40% di tutto il traffico su Internet sia generato da questi programmi. In pratica, su 10 sessioni utente su un qualsiasi sito web, quattro non sono riconducibili ad operazioni eseguite da esseri umani, ma ad automi che eseguono operazioni di vario genere e impatto sui siti web pubblici e privati di tutto il mondo.

Quale è il perché di tale successo? Molto semplice, perché i BOT possono fare tante cose, bene e velocemente: possono interagire con le pagine Web, inviare moduli, eseguire azioni, scansionare testi o scaricare contenuti. Possono accedere a video, pubblicare commenti e twittare su piattaforme di social media. Con alcuni BOT, noti come chatbot, si possono intrattenere vere e proprie conversazioni. Ci sono BOT che eseguono dei servizi utili ai clienti, e altri che servono ad ottimizzare i risultati delle ricerche su Internet. Tuttavia, accanto a questi BOT "buoni", ce ne sono altrettanti cattivi: i BOT sono in grado ad esempio di eseguire lo scraping o scaricare contenuti da un sito Web, rubare le credenziali degli utenti, inondare di contenuti spam le caselle di posta di qualche malcapitato oltre ad eseguire altri tipi di attacchi informatici come quelli descritti precedentemente.



Impatti sulle aziende

Generalmente, quando si sente parlare di BOT, si pensa, come nel caso dell'attacco descritto, agli impatti di sicurezza che gli stessi possono avere. E qui il mondo si divide sostanzialmente in due: da una parte c'è chi crede che il proprio sito non desti interesse per alcun possibile attaccante, quindi "perché preoccuparsi?". Dall'altra c'è invece chi per varie ragioni ha una consapevolezza maggiore in ambito di security, ma che vede il problema dei BOT solo dal punto di vista della security, ovvero "ho implementato delle contromisure avanzate di sicurezza, quindi sono al riparo dai BOT". In entrambi i casi ci troviamo di fronte ad una visione piuttosto limitata del problema. Tanto per cominciare i BOT hanno un impatto per tutte le aziende, grandi e piccole, in tutti i segmenti di mercato. Far parte di una categoria Small-Medium-Business o avere un portale che gestisce poco traffico non significa essere al riparto dai BOT. Allo stesso tempo, aver introdotto un'architettura di security ben progettata e configurata non è sempre sufficiente a respingere un attacco lanciato dai BOT.

Uno degli effetti più nocivi dei BOT non riguarda però la mera compromissione di informazioni o dell'operatività di un servizio, quanto l'impatto negativo in immagine che l'azienda subisce verso i propri clienti. Perderne la fiducia, per un'organizzazione di qualsiasi dimensione, è un danno molto difficile da recuperare e che impatta in maniera significativa il business.

Gli attacchi basati su BOT sono purtroppo un veicolo molto potente per questo tipo di situazioni e una non corretta gestione di questa problematica espone le organizzazioni verso un rischio di immagine che molto spesso è sottovalutato rispetto ai danni significativi che può arrecare.

Alcuni esempi di attacchi

Abbiamo detto che i BOT possono svolgere una moltitudine di operazioni sui siti target, con impatti in molti casi significativi. Ecco alcuni esempi:

1. Una compagnia aerea low cost ha utilizzato il BOT management per bloccare gli scrapers di una compagnia competitor che utilizzava dei programmi per effettuare la scansione automatica del sito, e basava le proprie tariffe su quelle offerte dalla concorrente.

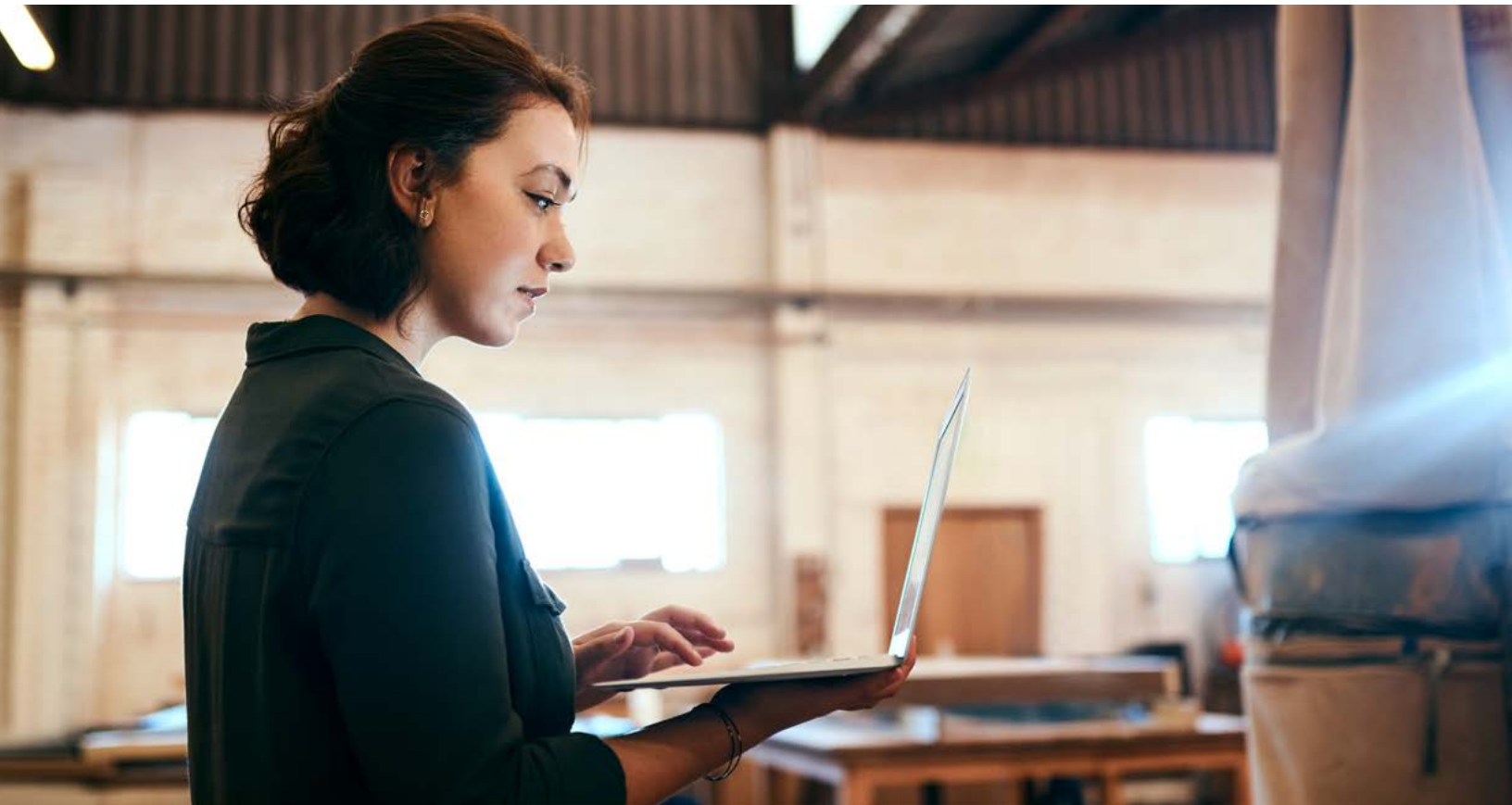
2. Molte aziende pagano profumatamente i click sui banner pubblicitari pubblicati su Internet. In questo contesto i BOT rappresentano un problema significativo per due ragioni: anzitutto effettuano dei click sui banner che le aziende pagano, sebbene tali click non porteranno poi a conversioni (ovvero ad acquisti, richieste di contatto, interesse per un prodotto o per un servizio, etc); in secondo luogo, i click dei BOT vanno a drogare le metriche di tool di analytics delle visite, fornendo dettagli sul “pubblico” di riferimento che non sono quindi attendibili.

3. Le aziende che utilizzano risorse nel cloud e che pagano infrastruttura e banda in misura dell’utilizzo realmente effettuato (pay-per-use), hanno una “bolletta” più salata a causa dei BOT: devono quindi dotarsi di infrastrutture più performanti per supportare non solo i propri utenti, ma anche i BOT che al tempo stesso causano un’occupazione di banda maggiore.

4. Come già evidenziato precedentemente, in alcuni casi, migliaia di BOT vengono comandati remotamente per effettuare attacchi DDoS con traffico del tutto lecito. In quei casi, l’unico modo per contrastare questo tipo di attacco è identificando l’origine della sessione e distinguendo gli utenti legittimi, dai BOT.

Come Citrix è efficace per contrastare i BOT

Come abbiamo visto diventa quindi imperativo dotarsi di soluzioni e metodologie che permettano una gestione efficace dei BOT, distinguendo quelli “benigni”, come ad esempio quelli dei motori di ricerca che aiutano la crescita del business, da quelli invece “nocivi”.



Citrix ADC (precedentemente noto come Citrix NetScaler) è un application delivery controller in grado di svolgere una moltitudine di funzioni tra le quali: Load Balancing, Access Gateway, Reverse Proxy, SSL Offloading, Proxy o Bridging, TCP Optimization, Caching, Web Application Firewall, L2 Extension, DDoS protection e Multi-Factor Authentication.

Una delle funzionalità più interessanti ed innovative presenti su Citrix ADC è proprio il BOT Management. Essa rileva i BOT malevoli (distinguendoli da quelli leciti) attraverso tecniche di Boot Trap, Rate Limiting, Device Fingerprinting, etc).

A questo proposito esistono varie metodologie che la tecnologia rende disponibile per la mitigazione degli attacchi BOT. Quando un client invia una richiesta, l'appliance valuta il traffico utilizzando le regole di rilevamento e permette di adottare un'azione di mitigazione idonea: drop, redirect, reset, log, captcha.

Per ulteriori dettagli: clicca qui

Anche l'implementazione di funzionalità di Multi-Factor Authentication (MFA) è uno strumento efficace per la prevenzione degli attacchi da BOT.

Citrix ADC può implementare in maniera rapida ed efficace questo strumento, anche per applicazioni che non ne prevedano nativamente l'uso, sia in modalità nativa (cioè senza bisogno di terze parti) sia integrando le soluzioni MFA - cloud e on-premise - più diffuse sul mercato.

E tutto questo senza richiedere nessuna modifica o riconfigurazione delle applicazioni da proteggere!

Cosa fare quindi?

Contattaci per verificare l'adeguatezza dei tuoi apparati (fisici, virtuali, multi-istanza) **e della licenza presente sugli stessi: se utilizzi già Citrix ADC, la soluzione al problema dei BOT potresti averla già in casa!**

Se invece non disponi di Citrix ADC, guarda come ottimizzare e rendere sicuri i tuoi servizi partendo da qui: https://www.citrix.com/products/citrix-adc/

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States