Aprile 2022

Il nuovo ABC per la sicurezza delle applicazioni

Dalle vulnerabilità delle API e i bot alla protezione del lato client

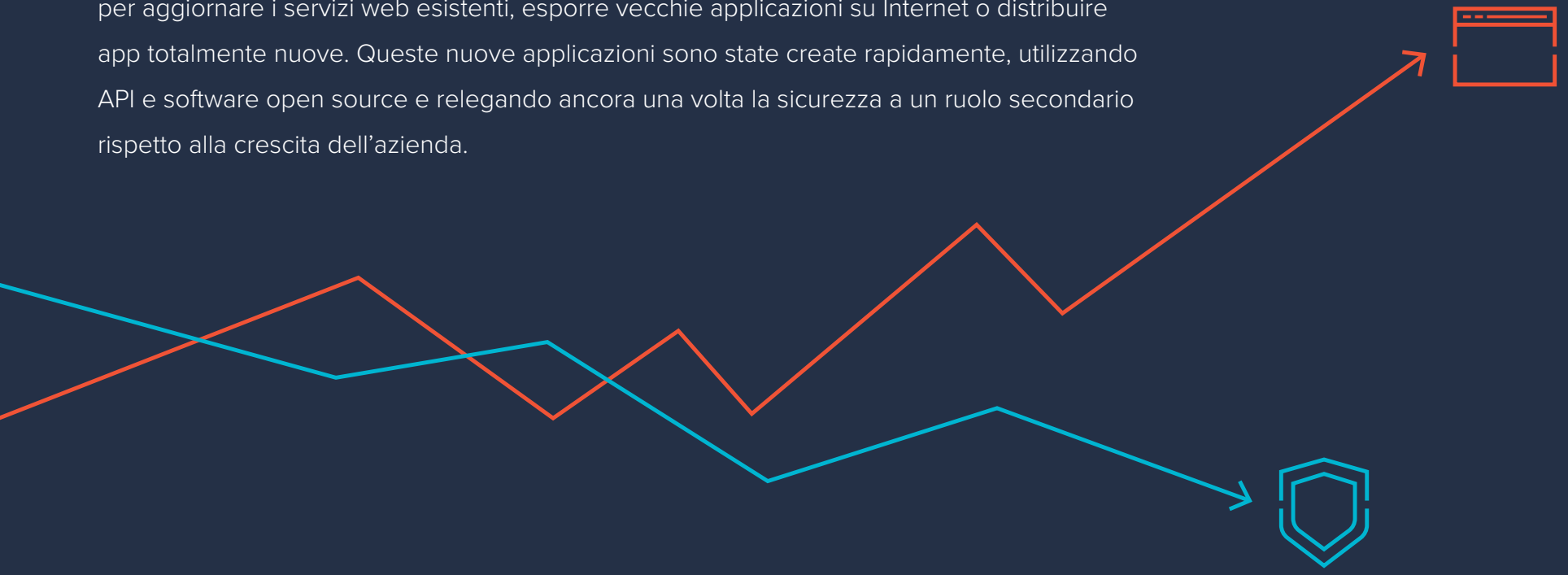
Barracuda

Indice

Barracuda

Introduzione: vettori di attacco nuovi e ancora più pericolosi

Le applicazioni sono gli elementi costitutivi del modo di operare delle aziende digitali e di coinvolgere i loro utenti e clienti. Il passaggio al lavoro a distanza nel 2020 ha incentivato l'importanza delle app web e molte organizzazioni hanno dovuto intervenire prontamente per aggiornare i servizi web esistenti, esporre vecchie applicazioni su Internet o distribuire app totalmente nuove. Queste nuove applicazioni sono state create rapidamente, utilizzando API e software open source e relegando ancora una volta la sicurezza a un ruolo secondario rispetto alla crescita dell'azienda.



Barracuda

Parlando di sicurezza delle applicazioni, le organizzazioni hanno sempre dovuto fronteggiare una serie di sfide. Da ormai diversi anni, le applicazioni sono uno dei principali vettori di attacco, un elemento che emerge dal report di indagine sulle violazioni di dati di Verizon e costituiscono anche una delle due principali motivazioni per cui le violazioni vengono messe in atto. A partire dai tradizionali attacchi diretti contro le applicazioni web, come SQL injection, cross-site scripting e command injection, questi attacchi si sono propagati anche alle API e alle app per dispositivi mobili.

Negli ultimi anni poi, le minacce alle applicazioni si sono moltiplicate e sono andati emergendo nuovi vettori di attacco ancora più pericolosi. I vettori di attacco oggi maggiormente sfruttati sono le vulnerabilità delle API, gli attacchi tramite bot automatizzati e gli attacchi lato client. In effetti, le persone che hanno risposto ai sondaggi condotti ai fini del report Barracuda The state of application security in 2021 hanno indicato gli attacchi bot, le vulnerabilità delle applicazioni web, gli attacchi alla supply chain del software e le falle di sicurezza delle API come le quattro principali motivazioni per cui, nelle rispettive organizzazioni, sono state possibili violazioni della sicurezza.

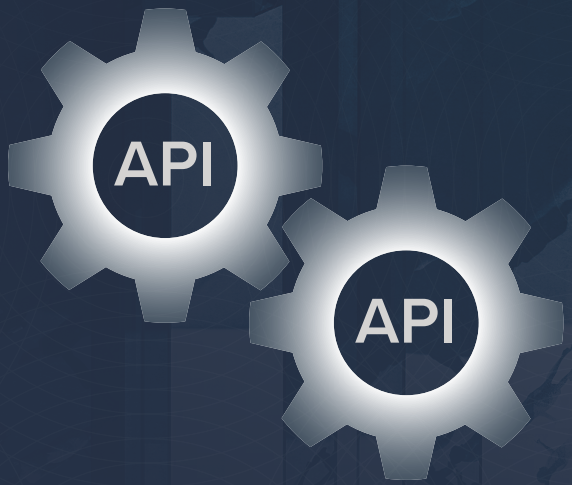
Il numero di vulnerabilità e violazioni attribuite ad attacchi alle API e al lato client è andato aumentando esponenzialmente e alcune di queste infrazioni, come quelle avvenute ai danni di T-Mobile e British Airways, sono anche finite sulla stampa, per i motivi sbagliati. Gli attacchi lato client, detti anche attacchi alla supply chain, sono stati inizialmente scoperti attorno al 2018 e sono anche definiti “Magecart”, perché in origine diretti contro negozi online basati su Magento. Gli hacker hanno dapprima identificato un JavaScript di terze parti, comunemente utilizzato nelle pagine di checkout. Dopo avere individuato questi file sorgenti, li hanno compromessi inserendo il loro codice di skimming delle carte. Quando un utente caricava il sito, veniva caricato anche il JavaScript divenuto pericoloso, che ne sottraeva le credenziali.

Gli attacchi bot hanno influito sulle aziende in altri modi. Uno dei principali è, ad esempio, l’acquisto automatizzato di articoli in edizione limitata allo scopo di rivenderli. Definiti anche attacchi di scalping, questi portano a carenze per gli acquirenti effettivi, come è accaduto nel caso della PlayStation 5. Da diverso tempo ormai i bot eseguono diversi tipi di attacchi, di cui i più pericolosi sono quelli legati al furto di account e gli attacchi DDoS.

In questo e-book vengono presi in considerazione più approfonditamente questi tre vettori di attacco cruciali, ovvero le vulnerabilità delle API, gli attacchi bot e gli attacchi lato client, si parla inoltre di come le organizzazioni possono colmare le lacune di sicurezza delle applicazioni che utilizzano e proteggersi da queste minacce in evoluzione.

A per la sicurezza delle API

Per molti anni, le API sono state utilizzate soprattutto in applicazioni aziendali di backend, per le comunicazioni da macchina a macchina. Oggi sono diffuse ovunque e presenti nella maggior parte delle applicazioni che tutti utilizziamo normalmente. Molte delle applicazioni web e per dispositivi mobili che usiamo per lavoro e per svago funzionano servendosi di API. Ormai costituiscono il cuore delle attività aziendali, sono alla base delle nuove piattaforme e consentono la trasformazione digitale.



Barracuda

Le organizzazioni si sono dedicate massicciamente a sviluppare “prima le API”, perché questo metodo consente loro di creare innovazione e uscire rapidamente sul mercato. Le API consentono agli sviluppatori di realizzare e rilasciare rapidamente nuove funzionalità per applicazioni web e dispositivi mobili, se utilizzate con prassi agili e DevOps, e consentono quindi tempi di fornitura veloci. Poiché il loro utilizzo è andato diffondendosi, le API sono diventate fondamentali in servizi di importanza cruciale per le applicazioni che abilitano e quindi hanno, a loro volta, sempre più accesso a dati critici.

La crescita delle API e il loro accesso diretto a dati critici le ha rese un bersaglio appetibile per gli autori degli attacchi. Le API sono fatte per l’automazione e questo rende molto proficuo per gli hacker trovare e sfruttare quelle non sicure. Gli attacchi automatizzati costituiscono per i criminali informatici un modo più semplice e rapido per esfiltrare dati rispetto alle applicazioni web. Le applicazioni basate su API inoltre codificano la propria logica aziendale nell’applicazione stessa, a differenza delle applicazioni tradizionali in cui la logica è nascosta nel server di backend. Questo comporta per i malintenzionati la possibilità di intercettare il traffico dell’applicazione e identificare gli endpoint API per attaccarli.

Il fatto che le API siano un nuovo grande bersaglio per gli hacker è confermato dal report BugCrowd PriorityOne del 2021, in cui si dice che le vulnerabilità delle API sono raddoppiate in soltanto un anno e che sono destinate ad aumentare più rapidamente, diventando nei prossimi anni uno dei principali vettori per le violazioni delle applicazioni.

Vulnerabilità delle API

raddoppiate

in un anno

Barracuda.

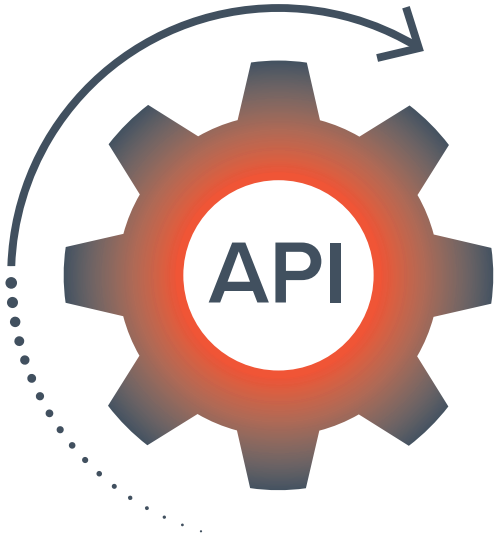
Esempio: esposizione dei punteggi di affidabilità creditizia dall'API Experian

Di recente, un ricercatore ha scoperto una grossa vulnerabilità delle API cercando online prestiti per gli studenti. Visitando il sito di una società finanziaria, ha visto che si poteva richiedere una valutazione dell'idoneità al prestito fornendo nome, indirizzo e data di nascita. Essendo un ricercatore, ha visualizzato il codice sottostante la ricerca e ha notato che inoltrava una chiamata all'API Experian. L'API che veniva utilizzata consentiva alla società finanziaria di inviare query automatizzate alla centrale dei rischi per reperire i punteggi di affidabilità creditizia.

Il ricercatore ha osservato che era possibile accedere direttamente all'API Experian senza utilizzare alcun tipo di sicurezza per l'applicazione, bastava inserire tutti zeri nel campo della data di nascita per estrarre il punteggio di affidabilità creditizia di chiunque. Ha quindi proseguito creando un pratico strumento per automatizzare le ricerche. Oltre ai punteggi di affidabilità creditizia, l'API restituiva anche quattro "fattori di rischio" per motivare l'attribuzione del punteggio.

Experian, contattata per questo problema, ha semplicemente rimosso l'accesso all'API da quest'unico endpoint.

Il pericolo derivante da questa esposizione è dimostrata dallo strumento creato dal ricercatore. Lui era un ricercatore e ha riferito la questione a Experian perché fosse risolta. Se questo endpoint API fosse invece stato individuato da un malintenzionato, avrebbe potuto sfruttarlo facilmente per procurarsi i punteggi di affidabilità creditizia di tutte le persone il cui nome e indirizzo sono di dominio pubblico, con la possibilità di causare danni significativi. Non è noto se la chiamata all'API desse luogo a un punteggio di affidabilità indicativo o vincolante e in che modo la visualizzazione del punteggio potesse influire sulla posizione creditizia di una persona.



Barracuda

Esempio: infrazione brute-force delle password di riunioni private su Zoom

Le riunioni su Zoom erano protette da una password numerica a sei cifre per impostazione predefinita. In base a questo, le password possibili per ciascuna riunione erano una su un milione. Un ricercatore ha scoperto che queste potevano essere forzate con un attacco brute-force, inondando Zoom di tentativi e altri attacchi simili.

Quando Zoom utilizzava password numeriche, un utente avrebbe potuto utilizzare il link della riunione per aprire la pagina web di richiesta della password e, a questo punto, dopo avere compilato i campi obbligatori e avere premuto Invio, avrebbe potuto osservare le interazioni con l'API di backend e scoprire la vulnerabilità.

Il fatto saliente di cui si è venuti a conoscenza su questo processo è che non era stata impostata alcuna limitazione della frequenza, pertanto il ricercatore ha potuto continuare a provare con le password e, dopo 43.164 tentativi in circa 29 minuti, con una frequenza di circa 25 password al secondo, è riuscito a scoprire la password corretta. Se nell'attacco fossero stati utilizzati più computer in parallelo, sarebbe stato possibile arrivare alla password molto velocemente.

Questa infrazione ha avuto implicazioni massicce. Dato il gran numero di enti governativi di alto livello e altre organizzazioni simili che utilizzavano Zoom, il problema avrebbe potuto causare gravi danni se dei malintenzionati fossero riusciti a entrare nelle riunioni e a intercettare quello che veniva detto. Il ricercatore ha fornito queste informazioni a Zoom, che ha implementato diverse modifiche per risolvere il problema.

Oltre alla mancanza di limitazioni della frequenza, è emerso un altro problema: l'assenza di controllo e monitoraggio degli accessi adeguati, che avrebbero potuto indicare in maniera relativamente semplice al team di Zoom che erano in corso quei tentativi.

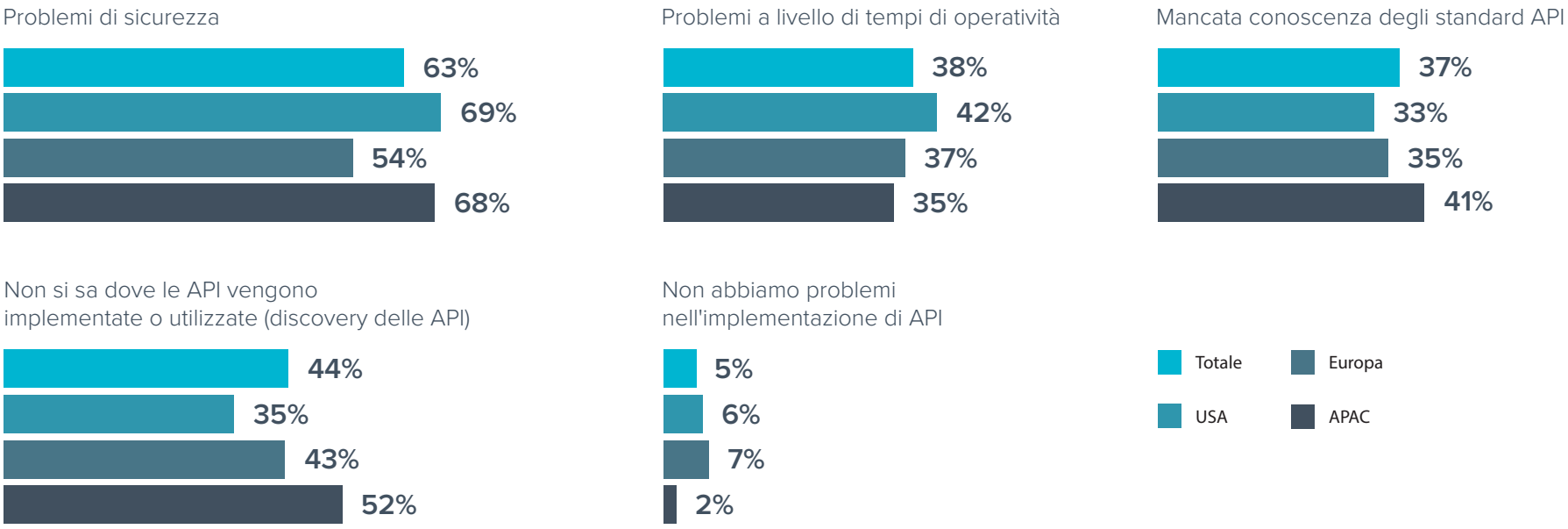
Barracuda

Che cosa dicono gli esperti di sicurezza delle applicazioni

Dato il notevole impatto che può avere una violazione delle API, è abbastanza ovvio che la loro sicurezza sia prioritaria per i difensori. In un recente sondaggio di Barracuda condotto su professionisti della sicurezza delle applicazioni è stato chiesto ai partecipanti di indicare le principali problematiche che affrontano nell'implementazione di API e la sicurezza è risultata predominante. Questo è confermato anche dal fatto che l' OWASP (Open Web Application Security Project) abbia rilasciato una Top 10 sulla sicurezza delle API, che consiste in una classifica delle vulnerabilità e dei rischi di sicurezza peculiari delle API.

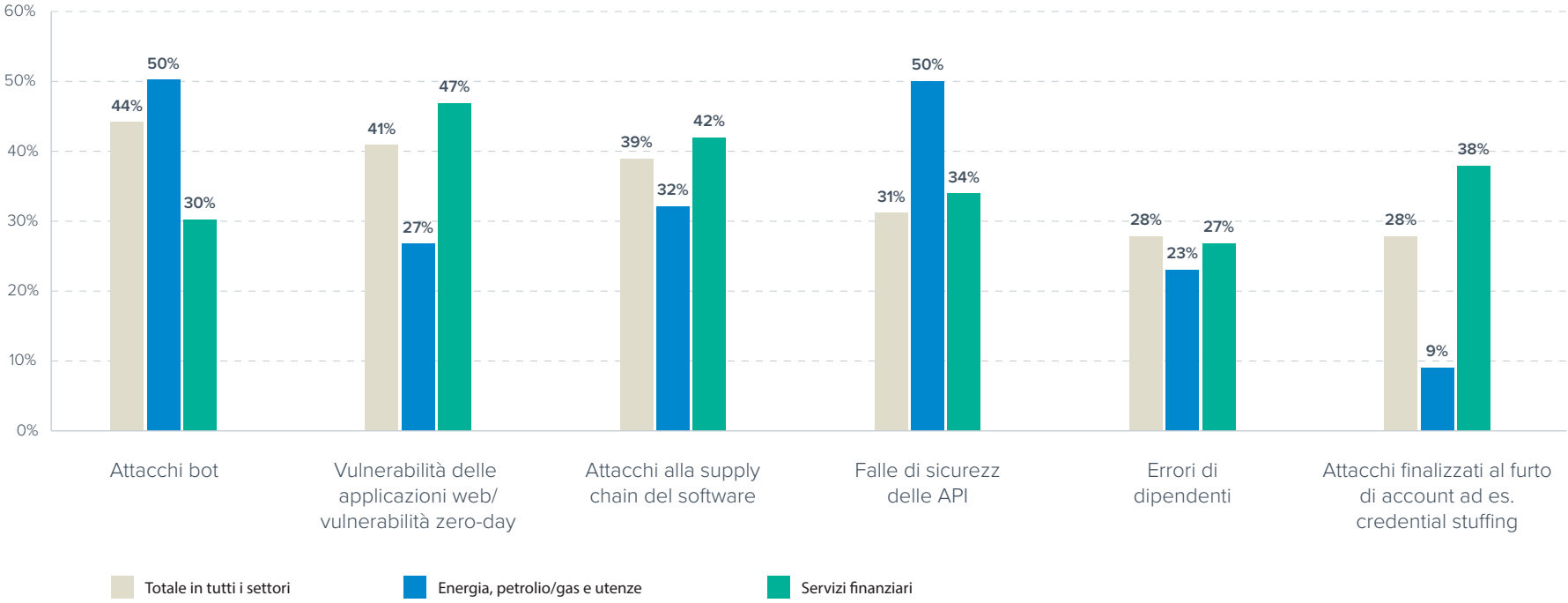
Quali sono le principali problematiche che la vostra organizzazione si trova ad affrontare nell'implementazione di API?

(n=728)



Quali dei seguenti elementi hanno contribuito alla riuscita delle violazioni della sicurezza che hanno sfruttato una vulnerabilità di un'applicazione della vostra organizzazione negli ultimi 12 mesi?

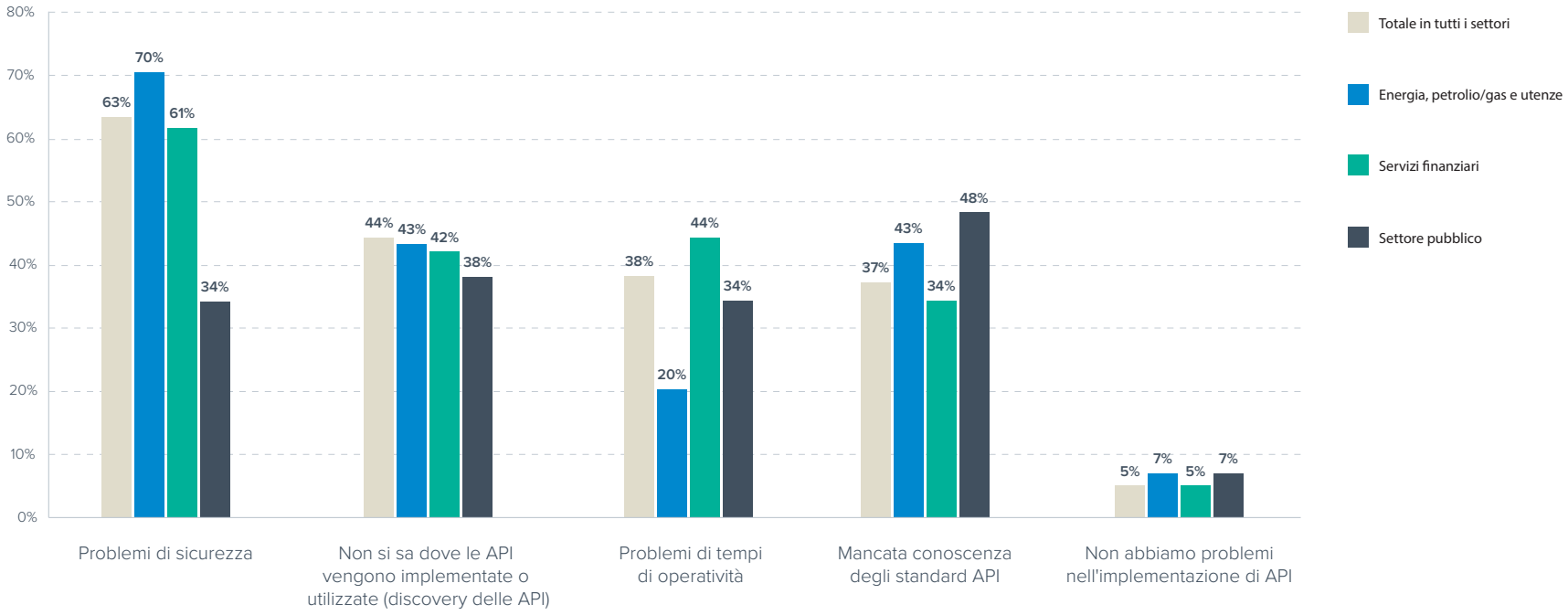
(n=541)



In base ai risultati del sondaggio, i settori dell'energia, del petrolio, del gas e delle utenze erano quelli più esposti a violazioni a causa di vulnerabilità delle API. Per quanto sulla stampa le notizie riguardanti il settore parlino soprattutto di attacchi ransomware mirati e di attacchi IoT, anche le API che vengono utilizzate, molte delle quali rivolte al pubblico, sono enormemente esposte alla minaccia di attacchi. Anche i partecipanti al sondaggio appartenenti al settore dei servizi finanziari, un campo in cui le API costituiscono la linfa vitale delle transazioni automatizzate, hanno indicato che le violazioni delle API sono per loro fra le principali cause di infrazione.

Quali sono le principali problematiche che la vostra organizzazione si trova ad affrontare nell'implementazione di API?

(n=728)

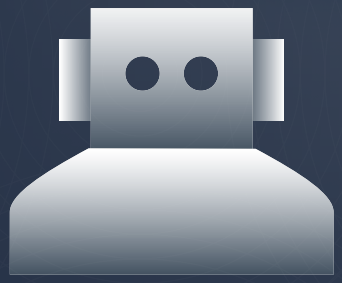


Il settore pubblico è quello che ha meno probabilità di avere problemi nell'implementazione delle API, in base alle risposte fornite. È interessante osservare che qui la questione principale è la "mancata conoscenza degli standard API" e che la sicurezza delle API è a un terzo di distanza, a differenza degli altri settori, che considerano pressoché unanimemente la sicurezza delle API come il problema principale. In confronto, i settori dell'energia, del petrolio, del gas e delle utenze, unitamente al settore manifatturiero, guidano il resto del drappello con il problema della sicurezza delle API.

Non stupisce che i partecipanti appartenenti a società di servizi finanziari fossero, fra tutti i settori, i più preoccupati dei tempi di operatività. Per i settori dell'energia, del petrolio, del gas e delle utenze, i partecipanti erano i meno interessati agli standard di conformità, il che è in qualche modo preoccupante, dato che, nella creazione di API, la conformità agli standard consente di migliorare la sicurezza.

B per la protezione dai bot

Negli anni scorsi, il traffico dei bot automatizzati è andato crescendo rapidamente. Una volta venivano usati principalmente dai motori di ricerca, oggi invece vengono impiegati per una varietà di utilizzi, sia buoni che cattivi. I bot buoni sono soprattutto crawler di motori di ricerca, bot di social network, crawler di aggregatori, bot di monitoraggio, ecc. Questi rispettano le regole del proprietario del sito web seguendo quanto specificato nel file robots.txt, rendono pubblici i propri metodi di convalida per stabilire che siano effettivamente chi dicono di essere e funzionano in modo da evitare di sovraccaricare i siti web e le applicazioni che visitano.

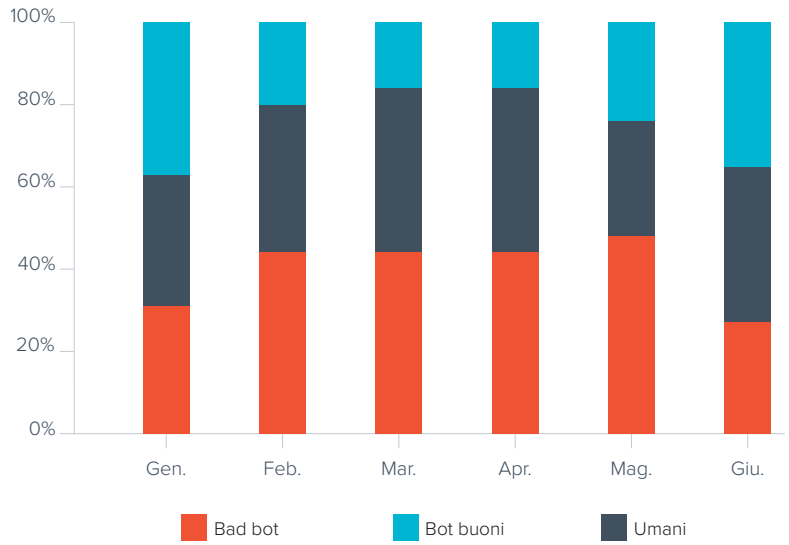


Barracuda

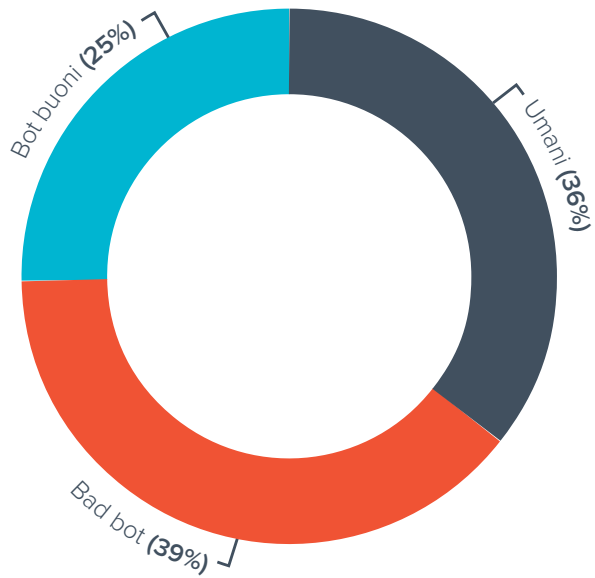
I bad bot sono costruiti in modo da eseguire varie attività dannose e possono consistere tanto in scraper di base che tentano di carpire alcuni dati da un'applicazione (e vengono facilmente bloccati) quanto in bot persistenti avanzati che si comportano quasi da umani e tentano di evadere il più possibile il rilevamento. Questi ultimi provano a mettere a segno attacchi di web scraping e price scraping, blocco delle scorte (inventory hoarding), furto di account, DDoS (Distributed Denial of Service) e altro ancora. I bad bot costituiscono oggi una parte significativa del traffico dei siti web ed è estremamente importante per le aziende individuarli e bloccarli.

Il traffico automatizzato costituisce circa i due terzi del traffico Internet, in base alle misurazioni delle tecnologie Barracuda effettuate nei primi sei mesi del 2021. Più o meno il 25% di questo traffico proviene da bot buoni noti, come i crawler dei motori di ricerca o i bot dei social network e di monitoraggio.

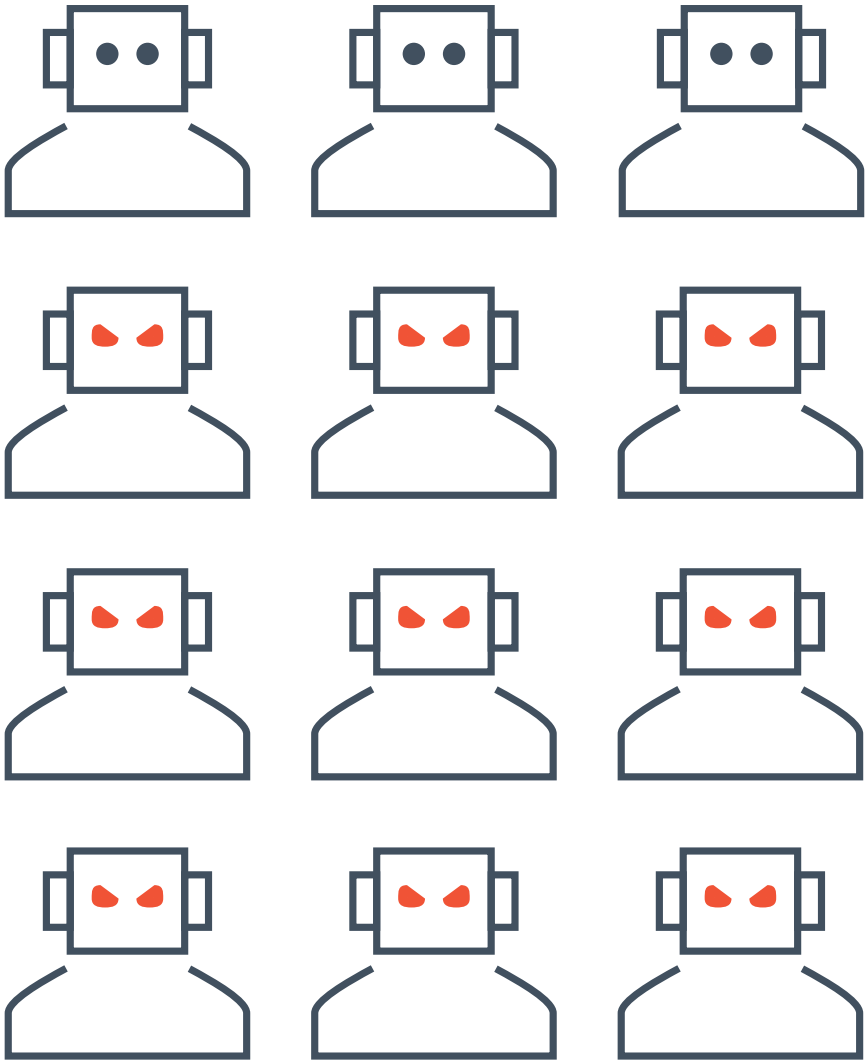
Distribuzione per mese



Distribuzione del traffico: bot/umani (gennaio – giugno 2021)



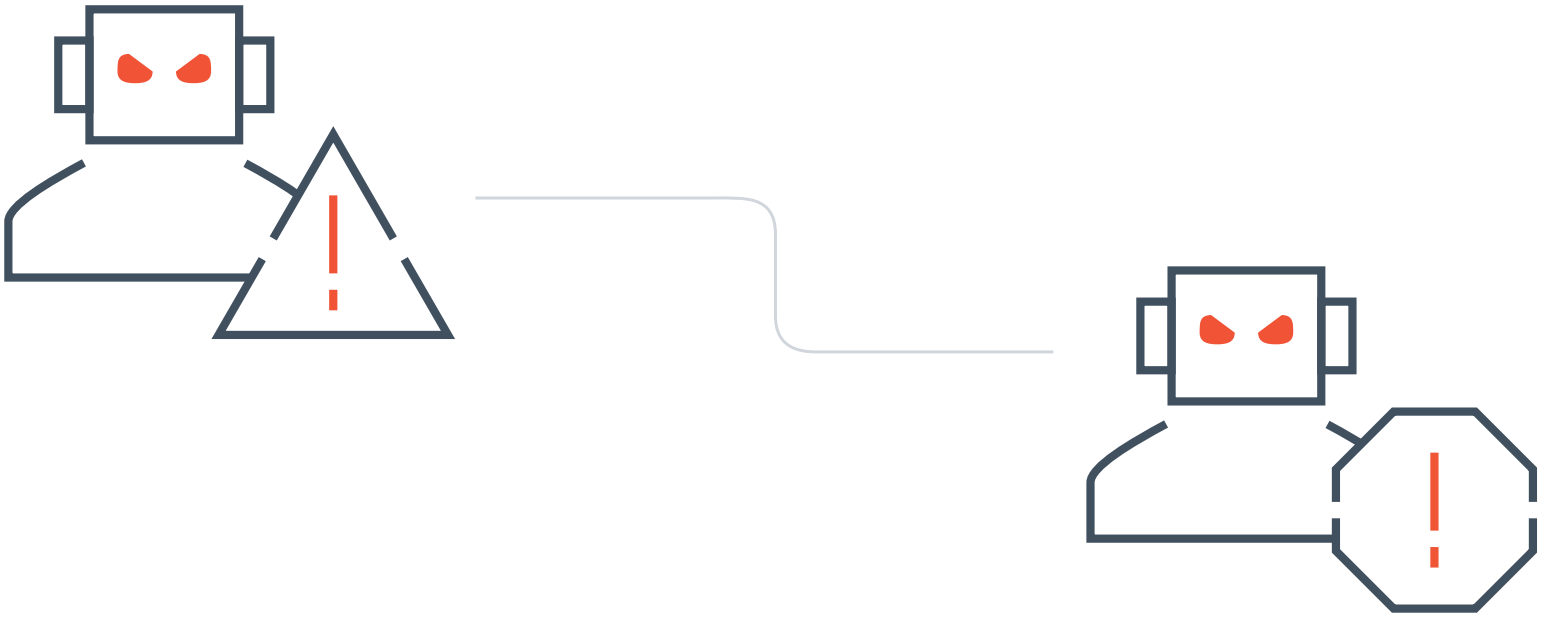
Oggi i bot sono altamente sofisticati e si comportano quasi come umani nella loro capacità di eludere molte difese. I sistemi standard impiegati per bloccarli, in particolare Google reCAPTCHA, sono per loro facilmente aggirabili. In effetti, le immagini utilizzate da CATPCHA sono più facili da risolvere per i bot che non per gli umani. Attorno ai bot intelligenti gravita un intero ecosistema: dalle persone che li creano, ai servizi che forniscono account Google con una “buona reputazione” per bypassare i test CAPTCHA, fino a servizi che offrono indirizzi IP residenziali (detti Resis) per eludere i blocchi basati sulla reputazione dell’IP e servizi di deposito (escrow) per evitare raggiri agli acquirenti di bot. Con l’aumento del numero di persone che si rivolge ai bot per fare soldi facili, come è accaduto con lo scalping della PlayStation 5 nel dicembre 2020, questi stanno avendo grande diffusione e diventano un grosso problema.



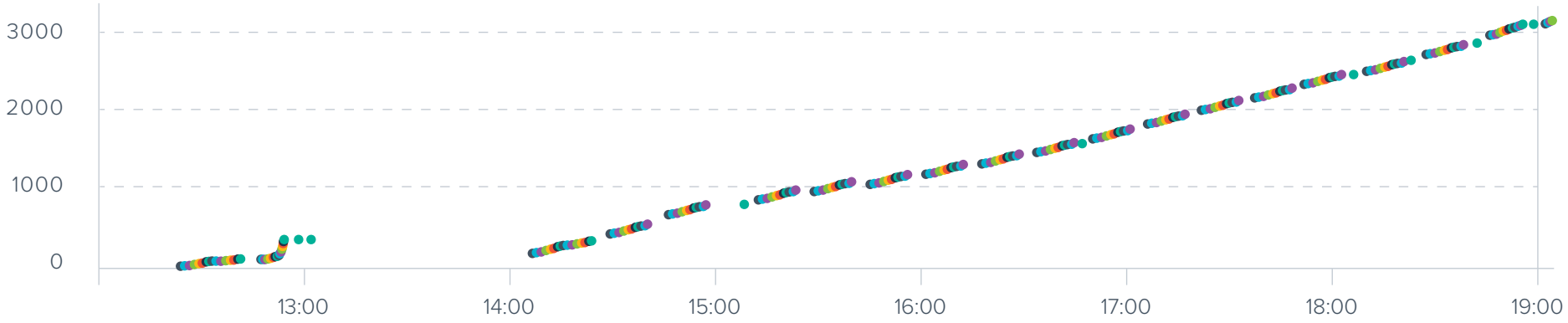
Esempio: price scraping di un negozio di e-commerce nell'Europa dell'Est

Barracuda ha rilevato e bloccato un tentativo di price scraping ai danni di un negozio di e-commerce con sede nell'Europa dell'Est. Il negozio stava praticando sconti su prodotti Apple e si sono verificati alcuni schemi sospetti nel comportamento del traffico, che proveniva da client con browser standard tramite diversi indirizzi IP residenziali locali. Tuttavia, questi indirizzi IP locali erano di provider di hosting VPS e ogni client accedeva soltanto a un set di pagine standard.

I malintenzionati sono stati smascherati attraverso questa correlazione e il tentativo di price scraping è stato bloccato.

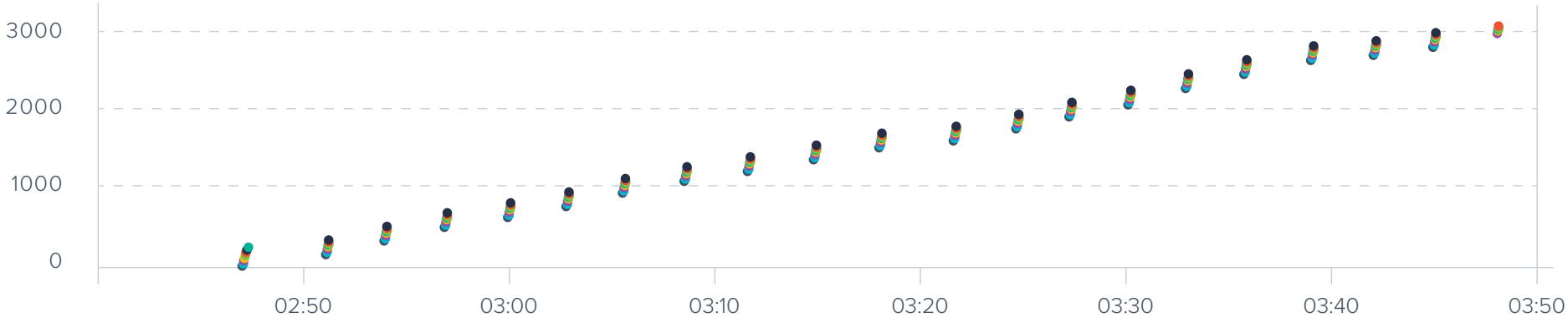


Schema di ripetizione di un bot di price scraping



I bot accedevano allo stesso set di URL dei prodotti più volte all'ora dopo il blocco della raffica iniziale.

Schemi di cambiamento dei bot per tentare di evitare il rilevamento

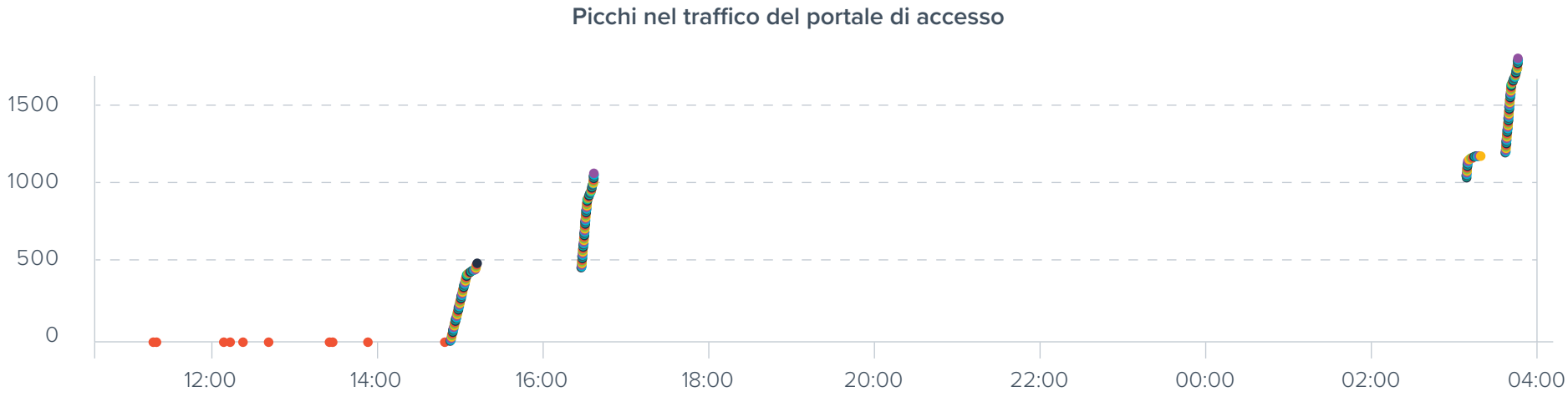


Bot che tentavano di accedere a un set più ridotto di pagine dei prodotti con diversi schemi di esplorazione più volte all'ora.

Barracuda

Esempio: tentativo di sovraccaricare il portale di accesso di un'azienda manifatturiera indiana

Il portale di accesso di un'azienda manifatturiera indiana stava assistendo a un traffico insolitamente elevato, proveniente in primo luogo da reti mobili, il che era strano ma non imprevisto per quel sito web. Tuttavia, mediante ulteriori analisi, il sistema ha stabilito che era più probabile che il traffico in ingresso provenisse da un browser desktop che impersonificava un dispositivo mobile connesso a un hotspot. I numerosi client che tentavano di sovraccaricare la pagina di login sono stati bloccati con successo e i tempi di risposta della pagina sono rientrati nella norma.



I primi pochi punti rappresentano un bot che fingeva di essere umano e diluiva gli accessi nel tempo. Dopodiché, sono presenti degli agglomerati, in cui ogni punto rappresenta un diverso client che tenta di accedere alla pagina di login.

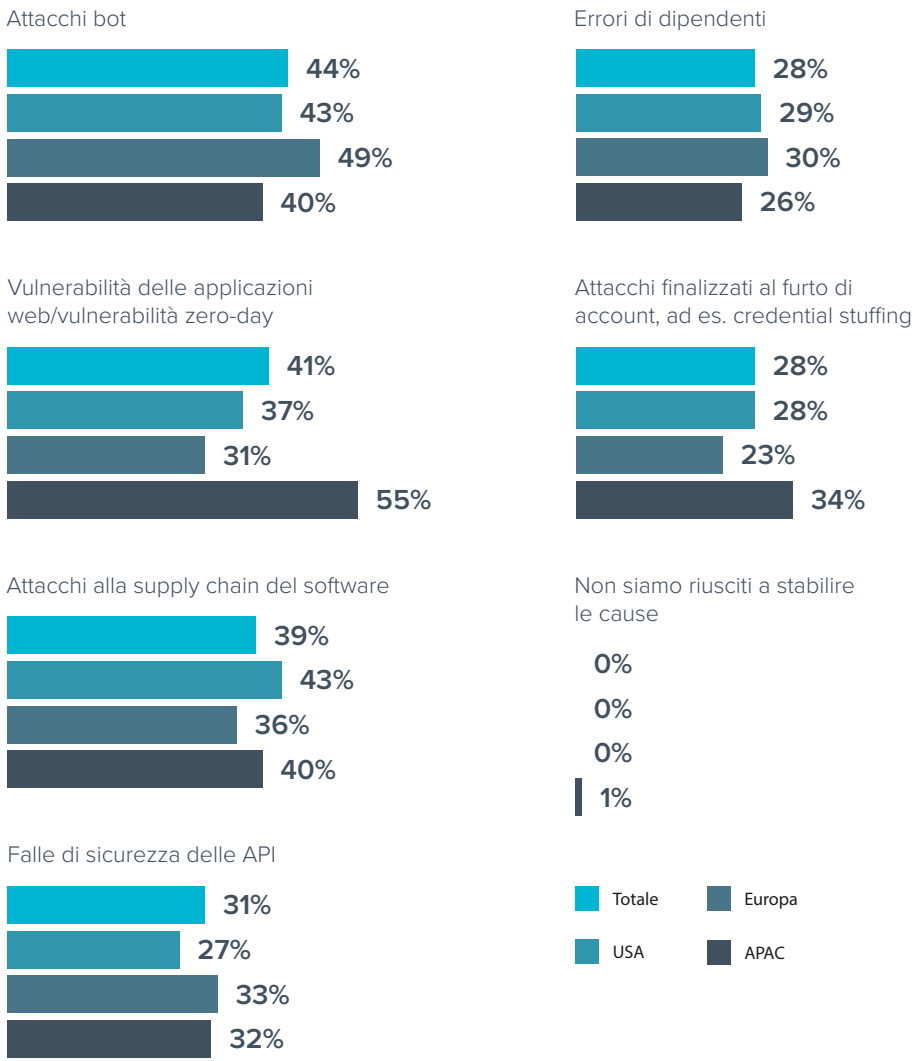
Che cosa dicono gli esperti di sicurezza delle applicazioni

Gli attacchi bot sono andati crescendo rapidamente negli ultimi anni e questo ha portato ad alcune compromissioni significative. Due anni fa, le più grandi minacce provenienti dai bot erano il furto di account o il credential stuffing e gli attacchi venivano spesso resi pubblici, così come la divulgazione dei casi di dumping delle credenziali da siti come LinkedIn.

In base al recente sondaggio di Barracuda condotto su professionisti della sicurezza delle applicazioni, negli scorsi 12 mesi, gli attacchi sferrati mediante bot sono probabilmente stati l'elemento preponderante nelle violazioni della sicurezza andate a segno derivanti da vulnerabilità delle applicazioni.

Quali dei seguenti elementi hanno contribuito alla riuscita delle violazioni della sicurezza che hanno sfruttato una vulnerabilità di un'applicazione della vostra organizzazione negli ultimi 12 mesi?

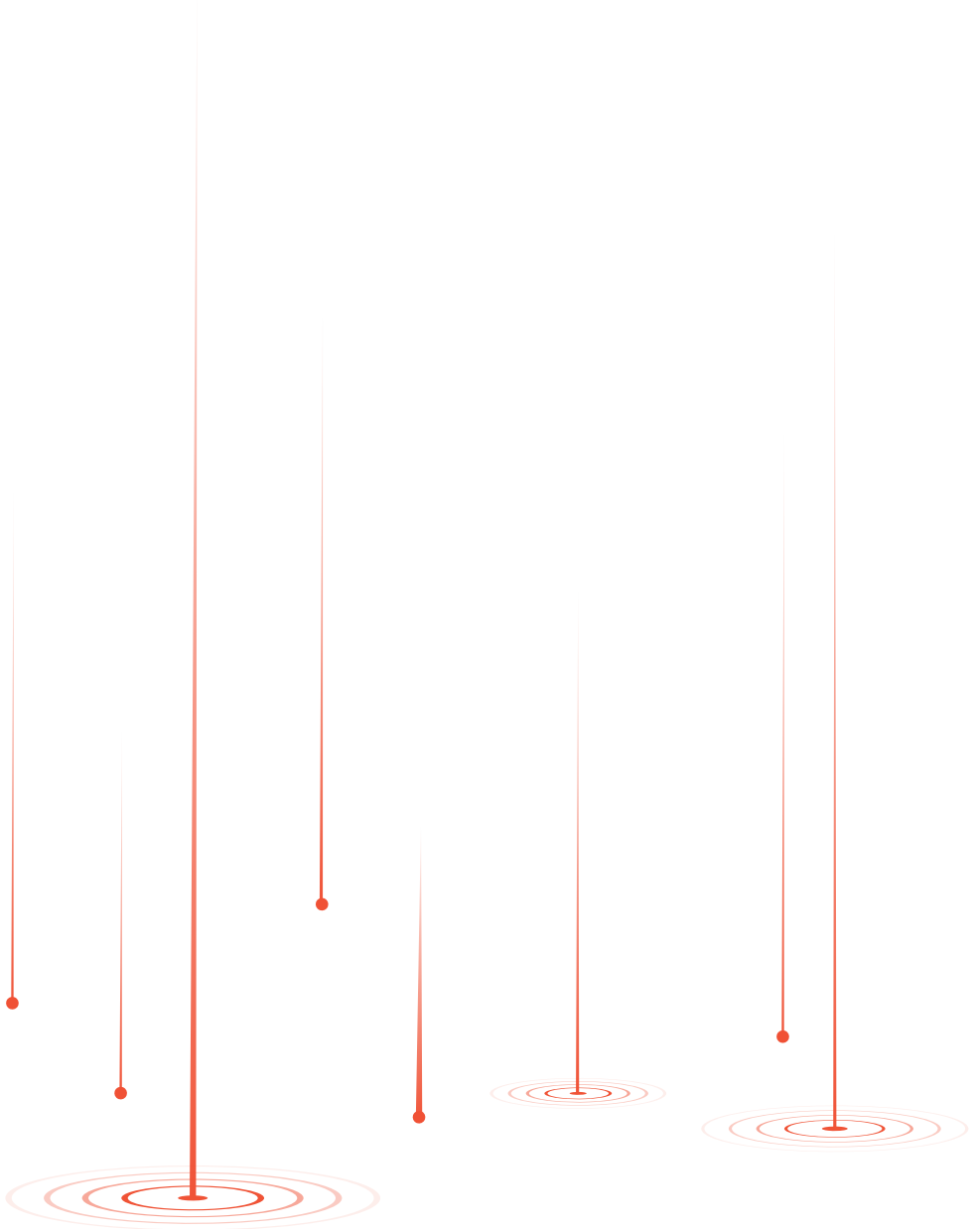
(n=541)



Data la diversificazione degli attacchi bot che prendono di mira le applicazioni, bloccarli diventa una lotta per chi vuole difendersi.

Con così tanta varietà in questo vettore di attacco, è evidente che siano molte le organizzazioni che cercano di proteggere le proprie applicazioni dai bot. Sebbene lo spam da questi generato sia più che altro un fastidio, viene spesso utilizzato per nascondere attacchi più dannosi, per cui va gestito, non ignorato. In base all'autenticità e alla frequenza dei messaggi di spam generati dai bot, può diventare difficile difendersi e la questione può trasformarsi molto facilmente da un'innocua seccatura in problemi operativi.

Anche i bot che eseguono lo spoofing di browser e app creano problemi ingenti. Queste falsificazioni possono essere semplici o complesse, da un utente che tenta di nascondere il suo vero browser a bot che eseguono versioni compromesse di app in click farm per pubblicare annunci fraudolenti o per altre finalità dannose.

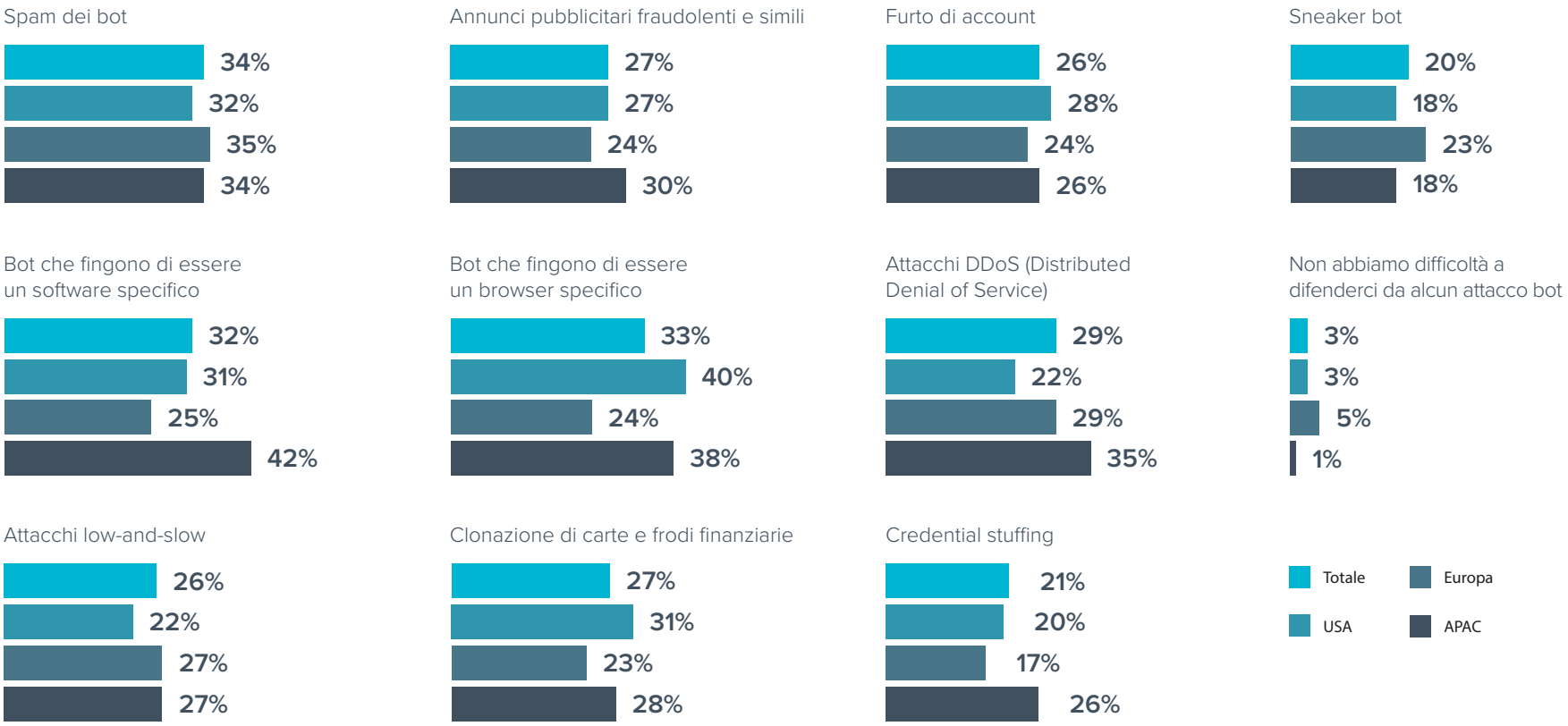


Barracuda

Tutti i bot, utilizzati in combinazione tra loro, incrementano le probabilità di successo di un attacco. Gli attacchi bot multivettoriali low-and-slow sono il cuore del problema e costituiscono probabilmente il principale elemento che ha contribuito alle violazioni messe a segno durante lo scorso anno.

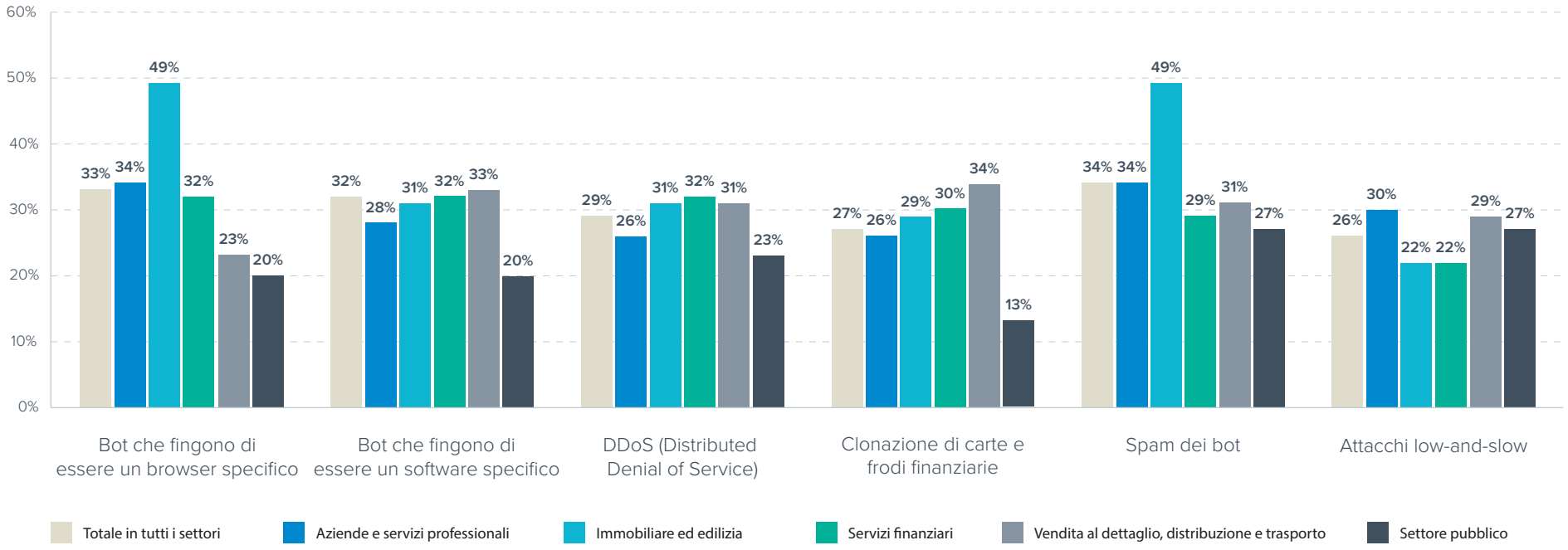
Da quali tipi di attacchi bot diretti contro le applicazioni la vostra organizzazione trova difficile difendersi?

(n=750)



Da quali dei seguenti tipi di attacchi bot diretti contro applicazioni della vostra organizzazione trovate difficile difendervi?

(n=750)



I partecipanti al sondaggio appartenenti al settore dei servizi finanziari hanno indicato tre tipi di attacchi bot come i più complessi contro cui difendersi: DDoS, bot che fingono di essere un software specifico e bot che fingono di essere un browser specifico. Questo tipo di frodi diventa un problema per le applicazioni finanziarie e gli autori degli attacchi si servono di versioni piratate per eseguire azioni malevole ai danni di queste organizzazioni. Gli attacchi DDoS comportano perdite finanziarie significative anche soltanto perché rendono i sistemi non disponibili.

Che la clonazione di carte e le frodi finanziarie si collochino al secondo posto nell'elenco è piuttosto interessante, in quanto ci si aspetterebbe che fossero la minaccia principale. Ciò dimostra che la prevalenza dell'accesso basato su browser o app per le organizzazioni finanziarie è ingente e continua a crescere.

In generale, i bot che fingono di essere un software o un browser specifico sono fra le cinque principali minacce in quasi tutti i settori. L'altra risposta interessante viene dal settore immobiliare e dell'edilizia, oltre che dal settore pubblico, che si dicono molto preoccupati per lo spam generato dai bot. Da ciò si evince che i siti immobiliari ricevono molto spam nelle loro inserzioni. Anche nel settore pubblico lo spam è un grosso problema. Ad esempio, fino a qualche anno fa, la quantità di voci "spam" nelle discussioni sulla neutralità della rete delll'FCC destava preoccupazione.

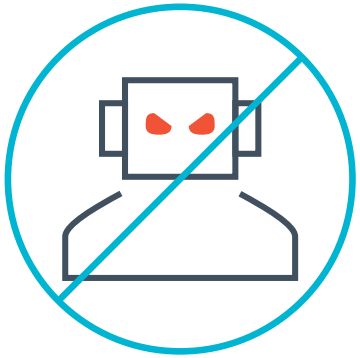
Il settore pubblico, unitamente a quello della vendita al dettaglio, alle aziende e ai servizi professionali, sono i più preoccupati per i bot low-and-slow. Le organizzazioni del settore pubblico in genere gestiscono molti download di file liberi (ungated) e divengono regolarmente bersaglio di malintenzionati che tentano di sferrare attacchi DDoS alle applicazioni. Anche le organizzazioni di vendita al dettaglio hanno molto da perdere dagli attacchi dei bot low-and-slow che tentano il furto di account, il price scraping, lo scalping e altro ancora.

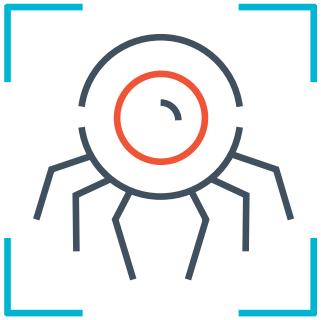
Prevenzione, rilevamento e identificazione sono funzionalità critiche per i fornitori che aiutano le organizzazioni a difendersi da attacchi basati su bot.

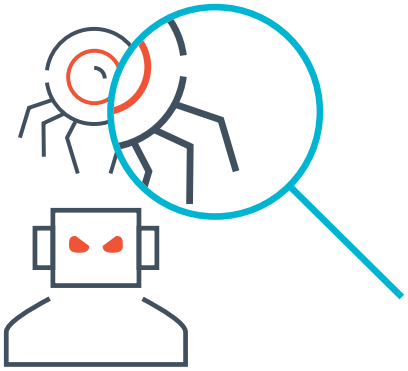
Barracuda.

Prevenzione, rilevamento e identificazione sono funzionalità critiche per i fornitori che aiutano le organizzazioni a difendersi da attacchi basati su bot.

Che le organizzazioni siano alle prese con bot che generano spam, tentano frodi o in grado di eseguire lo spoofing di software e browser, necessitano urgentemente di miglioramenti per difendersi da questo vettore di attacco. Dopo tutto, nell'ultimo anno, i bot sono stati i contributori più prolifici al successo delle violazioni ai danni delle applicazioni. Secondo i partecipanti al sondaggio, le aree su cui concentrarsi con le soluzioni di sicurezza per respingere i bot sono essenzialmente tre: prevenzione delle frodi, rilevamento dello spam e identificazione dei bot.



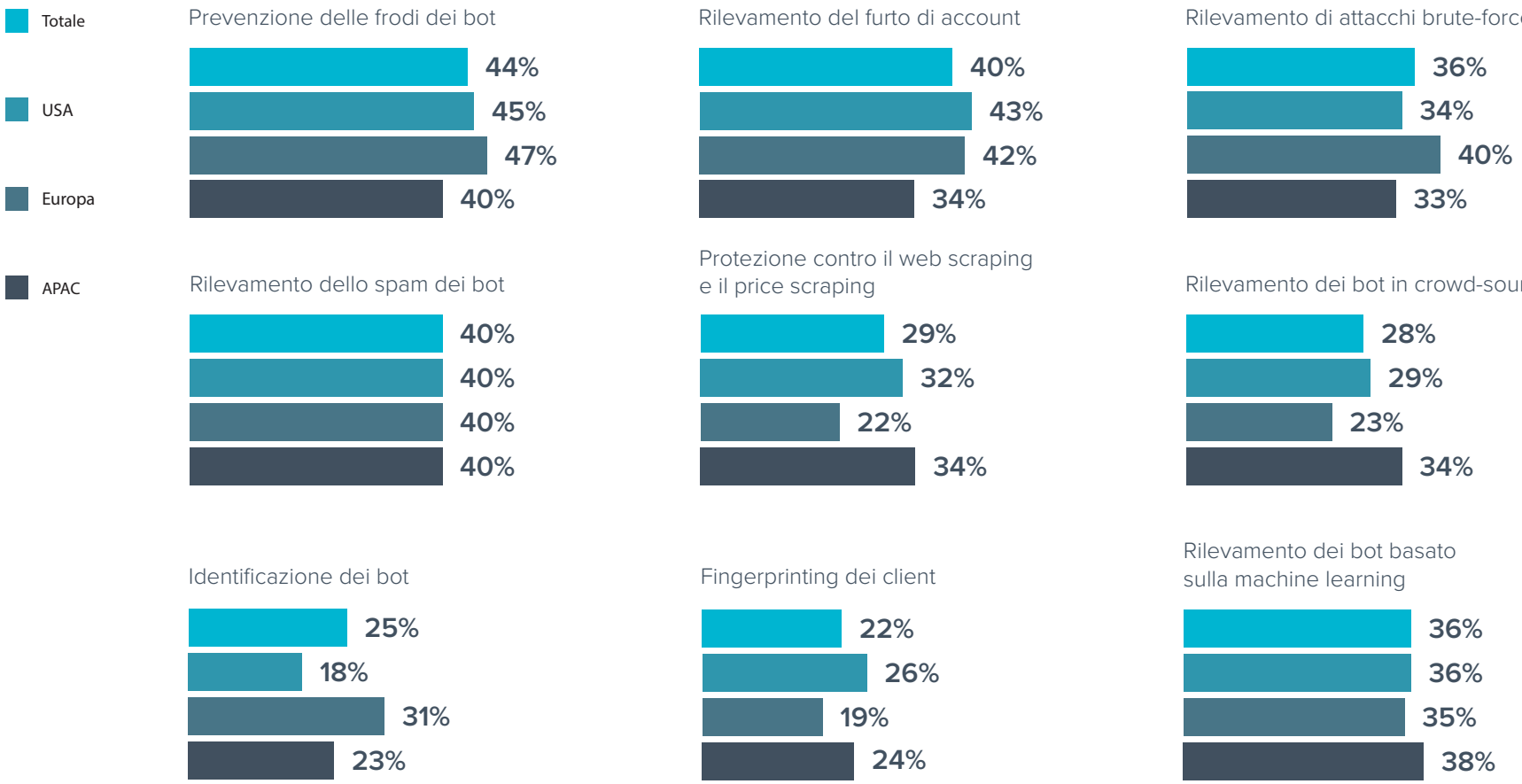




Questo genere di funzionalità sarebbe di importanza cruciale per difendersi da molti tipi di attacchi, ma se un fornitore fosse in grado di concentrarle tutte in un'unica soluzione, le capacità di proteggersi dai bot esistenti di molte organizzazioni ne sarebbero migliorate oltre misura.

Quali funzionalità sarebbero più importanti per la vostra organizzazione nella scelta di una soluzione di sicurezza da impiegare per la difesa delle applicazioni dagli attacchi bot?

(n=750)



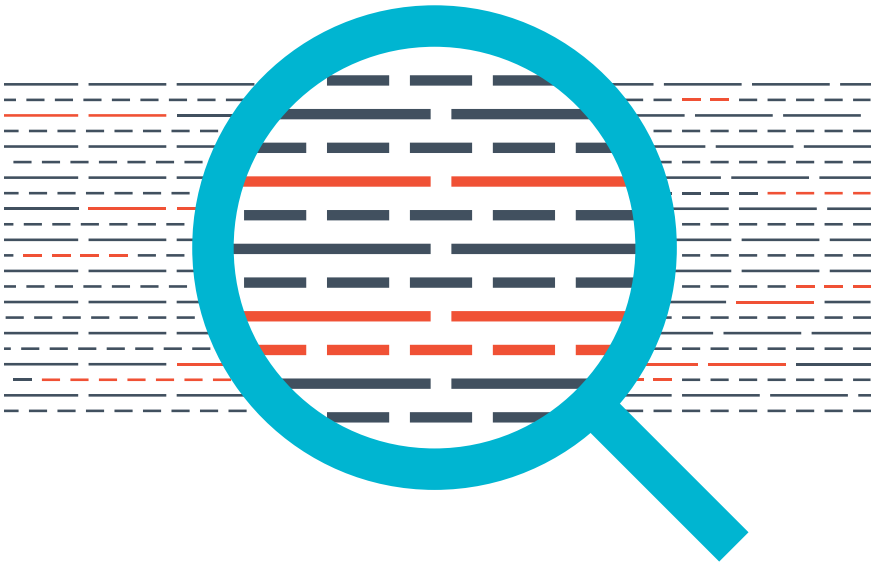
C per la protezione del lato client

Negli anni, è andata emergendo una moltitudine di nuove vulnerabilità specifiche legate al web, come il dirottamento dei clic (clickjacking) e il cross-site scripting (XSS), molti dei quali si manifestano sul lato client. E purtroppo sono ancora in auge le vulnerabilità del lato client che consentono l'iniezione, già presenti da oltre un decennio.

Gli attacchi lato client, detti anche attacchi alla supply-chain o Magecart (il cui nome deriva dall'applicazione di shopping Magento che era stata presa di mira in origine), sono difficili da rilevare e da bloccare.

Barracuda

Dagli esordi del web, avvenuti verso la fine degli anni ‘80, le app si sono evolute in modo continuo per soddisfare la nostra insaziabile fame di tutto ciò che è Internet. Questo cambiamento ha avuto luogo non solo dal lato server ma anche dal lato client (ovvero il browser). Proprio come i contenuti dinamici hanno sostituito quelli statici, le applicazioni a pagina unica hanno sostituito il semplice rendering basato su JavaScript per fornire un’esperienza più adatta allo scorrimento su telefoni e tablet. Dato che una quantità crescente di logica delle applicazioni sta passando al lato client, anche i malintenzionati hanno spostato la loro attenzione su questo lato. Gran parte di questa logica del lato client viene implementata utilizzando codice open source o di terze parti e, nel processo, la sicurezza finisce per essere messa da parte.



E quindi perché gli sviluppatori utilizzano codice di terze parti? Ebbene, per farla semplice, senza questo il web così come lo conosciamo oggi non sarebbe possibile. Le moderne pagine web comprendono decine, se non centinaia, di script esterni di terze o quarte parti. Si possono utilizzare strumenti come webpagetest.org per vedere quanti script di terze parti sono presenti in una data pagina web, e sono tanti. Questo approccio è accettato nello sviluppo web perché l’alternativa è impensabile: bisognerebbe reinventare migliaia di righe di codice. Il problema è l’affidabilità: uno script che oggi va bene domani potrebbe essere compromesso. Gli hacker prendono di mira le origini che ospitano questo codice di terze parti perché compromettendolo possono trasformare in una vittima ogni applicazione che lo utilizza.

Dato che il codice che viene modificato in modo da diventare dannoso è di terze parti, molti dei proprietari delle applicazioni non si accorgono che gli script sono stati compromessi, se non molto più avanti nel ciclo. Gli script stessi vengono caricati da altre origini, come reti CDN e repository di codice, non sono in genere forniti direttamente al browser dal sito web, e questo implica la difficoltà di rilevarli e bloccarli con gli strumenti e le prassi attuali.

Esempio: attacco alla supply-chain di British Airways

Nel 2018, una compromissione della supply-chain ha dato luogo alla violazione dei dati di un numero di clienti di British Airways compreso fra 380.000 e 500.000. Questa infrazione ha avuto come esito la perdita dei dati personali e di pagamento degli interessati.

Si è trattato di uno degli attacchi Magecart di più alto profilo del momento. Magecart è un gruppo che è stato scoperto nel 2016, dedito all'esecuzione dello skimming dei dati delle carte di credito online. Iniettavano script in grado di sottrarre specificamente i dati dai moduli di pagamento online, che poi utilizzavano per sé o vendevano ad altri criminali informatici.

In questo caso, il gruppo Magecart ha modificato uno specifico JavaScript utilizzato dalle app web e per dispositivi mobili di British Airways denominato Modernizr, integrandovi una piccola funzione che veniva eseguita al termine dello script. Al momento dell'esecuzione, la funzione raccoglieva i dati inseriti nel modulo di pagamento e li inviava a un sito web di terze parti gestito dal gruppo criminale. Si è così prodotta una grande esfiltrazione di dati e a British Airways è stata inflitta una multa di 20 milioni di sterline, che al momento era la massima multa mai comminata nel Regno Unito (ridotta dagli originali 183,39 milioni di sterline a causa dell'impatto economico della pandemia sul settore dei viaggi e le linee aree).

Clienti interessati dalla **violazione di dati**

380-500.000

Multa inflitta a British Airways

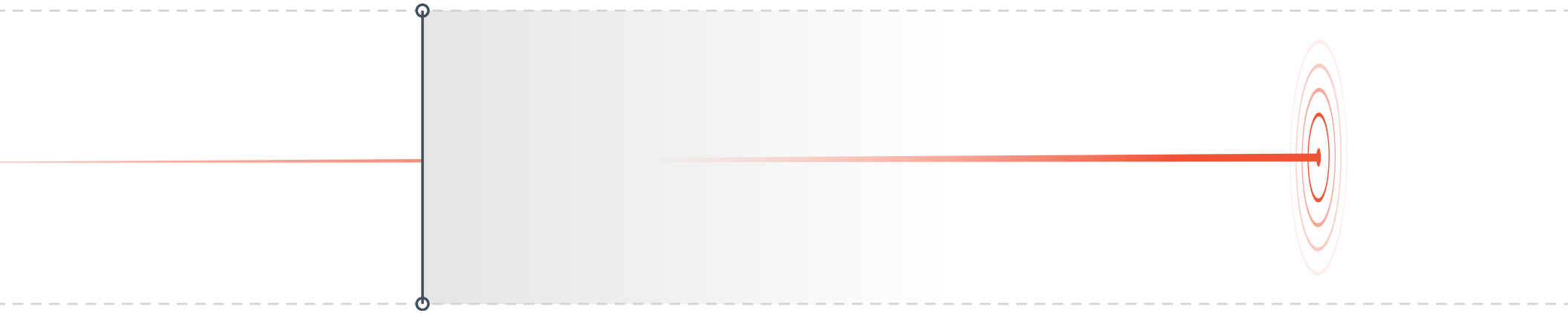
£20 Milioni

Barracuda

Esempio: Visa avverte della presenza di uno skimmer online

In settembre 2020, Visa ha emesso un avviso riguardante un nuovo skimmer online, denominato Baka, che veniva utilizzato in attacchi lato client. Questo skimmer impiegava meccanismi interessanti per evitare di essere rilevato. Al momento dell'esecuzione, veniva caricato dinamicamente nella memoria della macchina client, per cui non poteva essere rilevato mediante la normale scansione o l'ispezione della pagina. Era progettato in modo da essere eseguito soltanto dalla memoria, per cui non se ne trovava traccia nell'archivio del browser. I creatori dello skimmer si erano dati molta pena affinché fosse completamente crittografato e difficile da identificare quando veniva eseguito su un sito web o in un'applicazione.

Quando è stato reso noto, lo skimmer era presente e attivo in molti negozi online ed era stato evidentemente creato da sviluppatori esperti, che l'avevano progettato espressamente per eludere il rilevamento il più a lungo possibile.



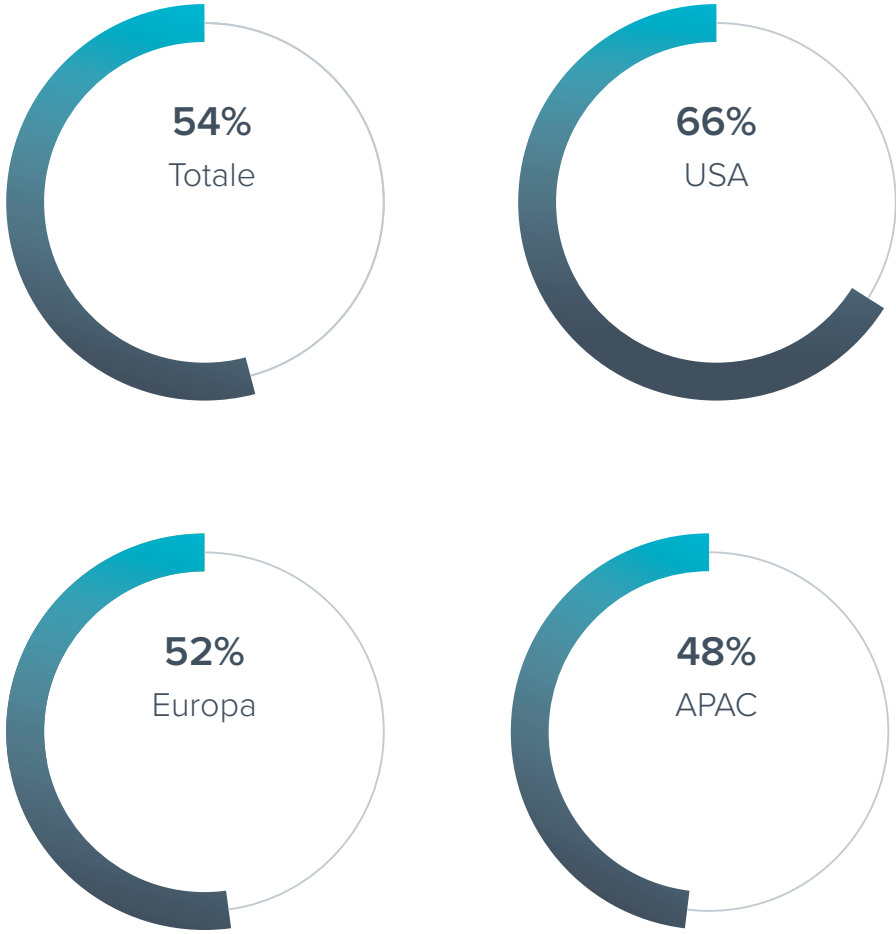
Che cosa dicono gli esperti di sicurezza delle applicazioni

L'uso di script di terze parti per le applicazioni web è molto diffuso e le organizzazioni utilizzano diversi metodi per fornire gli script a un browser.

Quando si tratta di sviluppo delle applicazioni web, la spinta all'efficienza è ancora una volta evidente dalle risposte fornite nel recente sondaggio di Barracuda condotto su professionisti della sicurezza delle applicazioni, dalle quali è emerso che più di metà delle organizzazioni utilizza script di terze parti già pronti per le applicazioni web. La sicurezza dev'essere tenuta in debita considerazione se si utilizza codice di terze parti e questo vale in particolar modo quando il codice viene fornito al browser direttamente da una piattaforma di sorgenti, come GitHub. Se il codice è stato manomesso, potrebbe già essere in preparazione un attacco alla supply-chain del software, come Magecart. Le organizzazioni devono stare attente a questo approccio nello sviluppo delle applicazioni.

Approssimativamente in quale percentuale delle applicazioni web della vostra organizzazione vengono utilizzati script di terze parti?

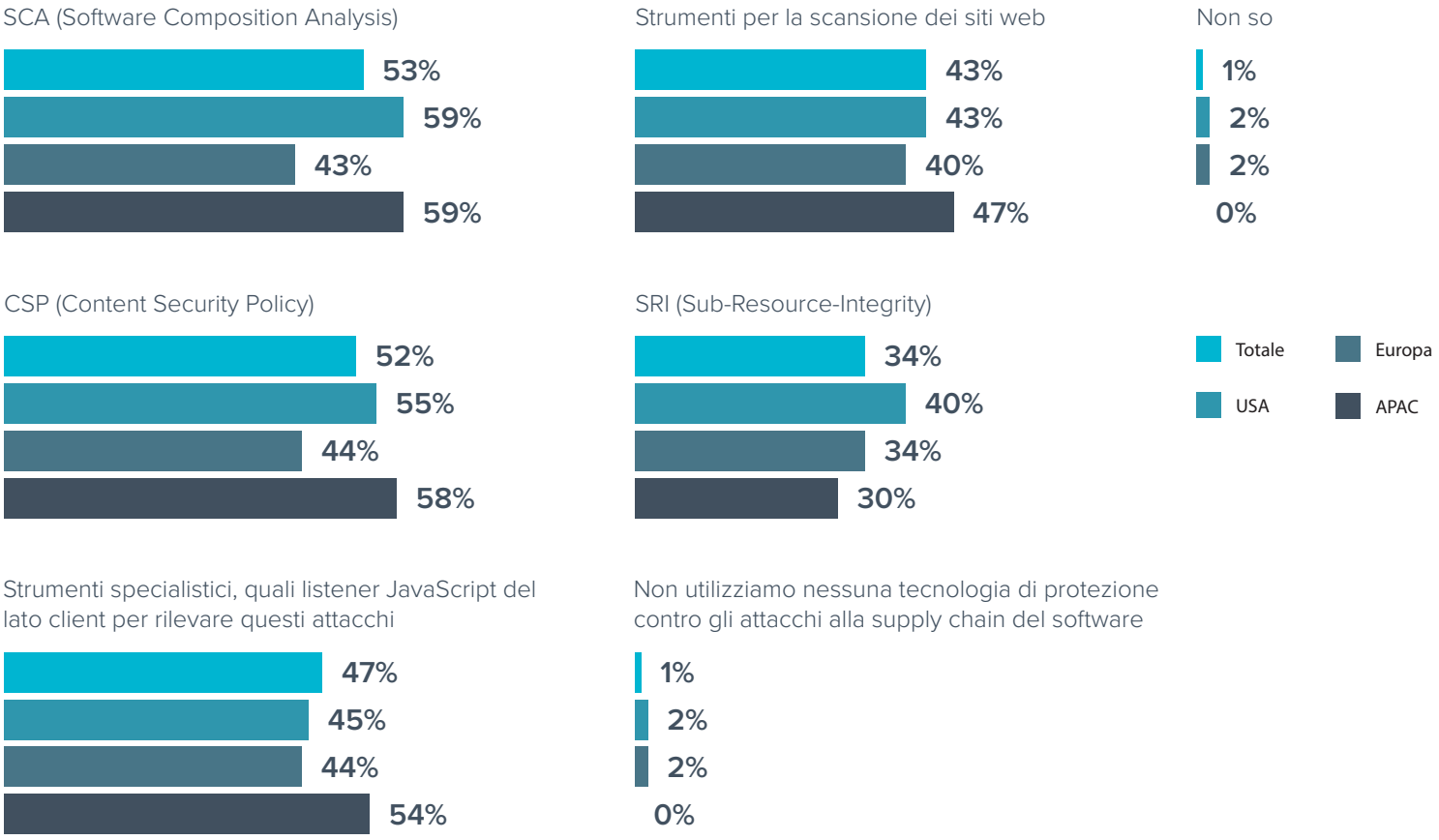
(n=750)



Per il contenimento degli attacchi alla supply-chain vengono adottate misure di protezione relativamente standard. Più che in altre regioni, i partecipanti al sondaggio con sede nei paesi APAC hanno detto di utilizzare strumenti specialistici, fra cui listener JS del lato client. Questi listener hanno maggiori probabilità di rilevare gli attacchi più avanzati rispetto agli strumenti per la scansione dei siti web. Questi strumenti costituiscono la quarta tecnologia più diffusa in questo elenco, ma sono facili da aggirare, come si è visto con lo skimmer Baka individuato da Visa. L'integrità delle risorse secondarie (SRI, Sub-resource Integrity) è difficile da impostare e da mantenere, e questa potrebbe essere una delle ragioni per cui non è molto considerata.

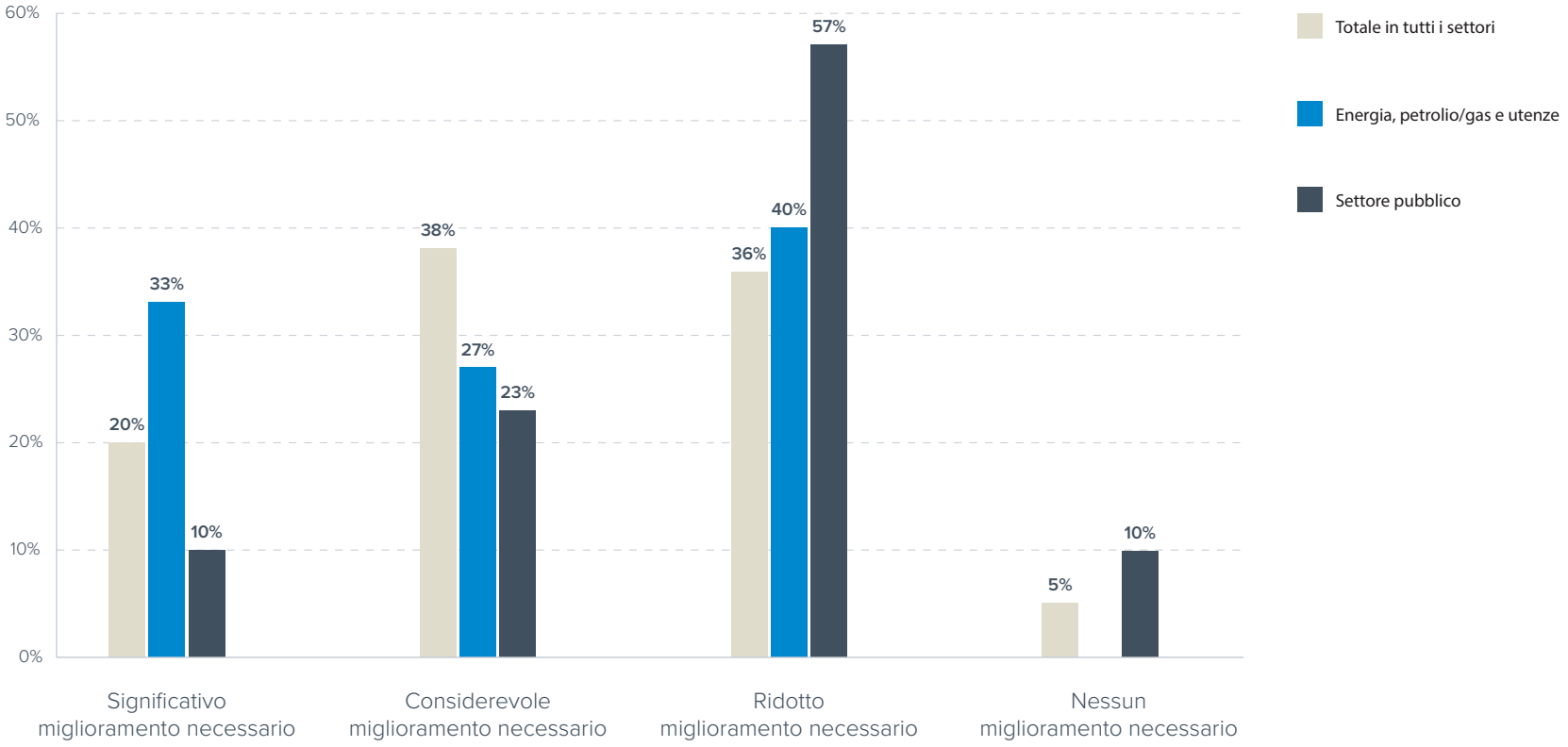
Quali tecnologie utilizza l'organizzazione per proteggersi dagli attacchi alla supply chain del software?

(n=750)



Quale livello di miglioramento pensate sia necessario nella vostra organizzazione per difenderla dagli attacchi alla supply chain del software?

(n=728)



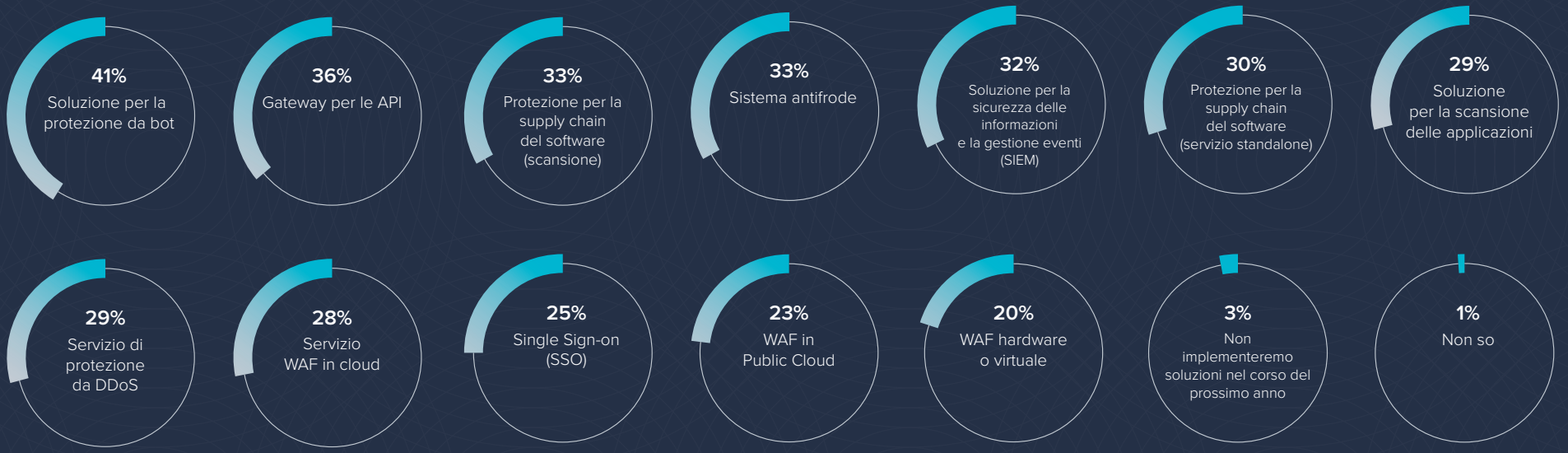
La maggior parte delle organizzazioni è combattuta sui miglioramenti necessari per la supply chain dei propri siti web. I partecipanti al sondaggio appartenenti al settore pubblico erano più inclini a dichiarare che occorrevano piccoli miglioramenti o nessun miglioramento alla loro protezione. Solo i settori dell'energia, del petrolio, del gas e delle utenze hanno indicato la necessità di miglioramenti significativi. Questo probabilmente è un riflesso del fatto che il vettore di attacco è emerso in tempi relativamente recenti e che l'impatto ancora non è pienamente apprezzato. Man mano che questi attacchi vengono scoperti, il vettore di attacco sarà sempre più noto.

Conclusione: come prepararsi al nuovo ABC per la sicurezza delle applicazioni

Le organizzazioni subiscono sempre più spesso violazioni attraverso le applicazioni web e le API. Man mano che proliferano nuove tecnologie, gli autori degli attacchi si adoperano per trovare nuovi modi di eludere le misure di sicurezza e infrangerle. Le API, i bot e il lato client sono i nuovi bersagli che hanno individuato per violare le applicazioni a scopo di divertimento o di lucro.

Quali delle seguenti soluzioni verranno implementate nella vostra organizzazione nel corso del prossimo anno?

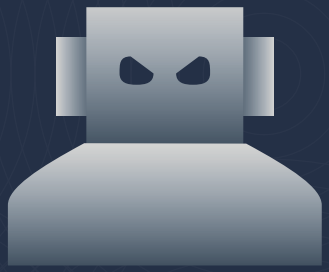
(n=750)



Barracuda

Nelle nostre ricerche riscontriamo che le organizzazioni sembrano comprendere questo concetto e che molte siano alla ricerca di nuove soluzioni da implementare nel corso del prossimo anno, ad esempio, protezione dai bot (41%), gateway per le API (36%) e protezione della supply chain del software (scansione) (33%).

È un buon segno che si stiano muovendo per colmare queste lacune ma, più aggiungono soluzioni, più la sicurezza delle applicazioni assume complessità. Per fornire una protezione efficace, una soluzione di sicurezza delle applicazioni deve essere una piattaforma in grado di proteggere i clienti da tutti questi vettori di attacco. Un approccio alla sicurezza delle applicazioni: basato su piattaforma fornisce una protezione potente dalle minacce sia tradizionali che emergenti, rimanendo nel contempo semplice da utilizzare e da gestire.



Informazioni su Barracuda

Barracuda si adopera per rendere il mondo più sicuro. Crediamo che tutte le aziende meritino l'accesso a soluzioni di sicurezza di livello enterprise cloud-first, che siano semplici da acquistare, implementare e utilizzare. Proteggiamo l'e-mail, le reti, i dati e le applicazioni con soluzioni innovative espandibili e adattabili lungo il percorso dei clienti. Oltre 200.000 organizzazioni di tutto il mondo si affidano a Barracuda per essere protette in modi per cui non sanno nemmeno di essere a rischio, per potersi concentrare sulla propria attività e salire di livello. Per ulteriori informazioni visitate il sito barracuda.com.