Abril de 2022

El nuevo abecé de la seguridad de las aplicaciones

Desde las vulnerabilidades de las API y los bots hasta la protección del lado del cliente

Barracuda®

Índice

Introducción: vectores de ataque más peligrosos y novedosos 1

A de seguridad de las API 4

Ejemplo: Exposición de calificaciones crediticias por la API de Experian 6

Ejemplo: Ataque de fuerza bruta a las contraseñas de las reuniones privadas en Zoom 7

Opinión de los profesionales de la seguridad de aplicaciones 8

B de protección frente a los bots 11

Ejemplo: Raspado de los precios de una tienda de comercio electrónico de Europa del Este 14

Ejemplo: Intento de sobrecargar el portal de inicio de sesión de una empresa de fabricación india 16

Opinión de los profesionales de la seguridad de aplicaciones 17

C de protección del lado del cliente 24

Ejemplo: Ataque a la cadena de suministro de British Airways 26

Ejemplo: Advertencia de la existencia de un skimmer en línea por parte de Visa 27

Opinión de los profesionales de la seguridad de aplicaciones 28

Conclusión: preparación de cara al nuevo abecé de la seguridad de las aplicaciones 31

Sobre Barracuda 33

Barracuda

Introducción: vectores de ataque más peligrosos y novedosos

Las aplicaciones son la base del funcionamiento de los negocios digitales y del modo en que estos interactúan con sus clientes y usuarios finales. Con el cambio al teletrabajo que se produjo en 2020, las aplicaciones web cobraron aún más peso, ya que muchas organizaciones tuvieron que cambiar de rumbo muy rápido y, para ello, actualizar sus servicios web, volver a ofrecer sus antiguas aplicaciones en Internet o implementar algunas completamente nuevas. En el acelerado desarrollo de estas nuevas aplicaciones, que se llevó a cabo mediante API y software de código abierto, se volvió a infravalorar la importancia de la seguridad para lograr la expansión del negocio.

Barracuda

Las organizaciones siempre han tenido que hacer frente a dificultades de todo tipo en lo que respecta a la seguridad de las aplicaciones. De hecho, las aplicaciones son uno de los vectores de ataque más comunes en las filtraciones de datos, algo que se lleva confirmando varios años en el informe Verizon Data Breach Investigation Report, y uno de los dos principales motivos de que se produzcan violaciones de seguridad. Los ataques lanzados tradicionalmente contra las aplicaciones web, como las inyecciones de código SQL, las secuencias de comandos en sitios cruzados y las inyecciones de comandos; ahora también ponen en el centro de la diana a las API y las aplicaciones móviles.

Las amenazas a las aplicaciones se han multiplicado en los últimos años y, ahora, han surgido vectores de ataque más peligrosos y novedosos. De entre todos ellos, las vulnerabilidades de las API, los ataques de bots automatizados y los ataques del lado del cliente son los que están experimentando un crecimiento más rápido. De hecho, los encuestados para nuestro informe El estado de la seguridad de aplicaciones en 2021 mencionaron los ataques de bots, las vulnerabilidades de las aplicaciones web, los ataques a la cadena de suministro de software y la seguridad deficiente de las API como las cuatro causas principales de las violaciones de seguridad sufridas por sus organizaciones.

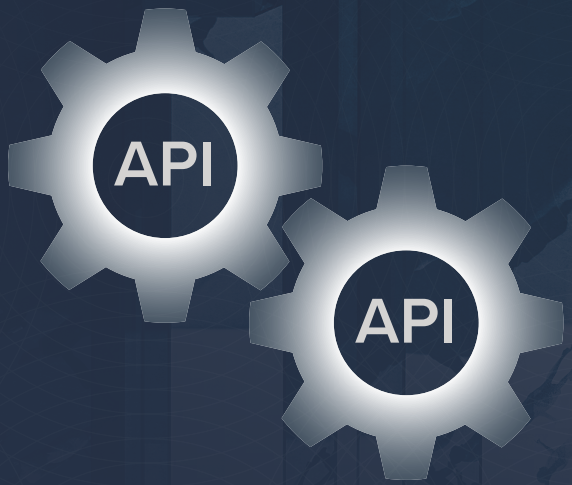
El número de vulnerabilidades y violaciones atribuidas a los ataques a las API y del lado del cliente ha aumentado exponencialmente; además, algunas de ellas, como las de T-Mobile y British Airways han acaparado los titulares por los motivos equivocados. Los ataques del lado del cliente, también conocidos como ataques a la cadena de suministro, se descubrieron hacia 2018 y recibieron el sobrenombre de Magecart, ya que, en un inicio, se lanzaban mayoritariamente a las tiendas en línea que operaban en la plataforma Magento. El modus operandi de los atacantes consistía en identificar código JavaScript de terceros, que por entonces se solía emplear en las páginas de pago, hackear estos archivos de código fuente e insertar su código de skimming de tarjetas. Así, cuando un usuario accedía al sitio, se cargaba el malintencionado código JavaScript y robaba las credenciales.

El impacto negativo de los ataques de los bots se ha manifestado de otras formas en las empresas. Por ejemplo, unos de los ataques más habituales son los ataques de scalping, es decir, la compra automatizada de artículos de edición limitada para su posterior reventa. El objetivo es provocar el desabastecimiento para los clientes reales, como ocurrió con la videoconsola PlayStation 5. Los bots llevan ya un tiempo acometiendo una amplia variedad de ataques, entre los que destacan la usurpación de cuentas y los ataques de DDoS, que son los más perjudiciales.

En este libro electrónico, se analizan en profundidad estos tres vectores de ataque principales, las vulnerabilidades de las API, y los ataques de bots y del lado del cliente, así como la forma en que las organizaciones pueden reforzar la seguridad de sus aplicaciones y protegerse frente a este tipo de amenazas en constante evolución.

A de seguridad de las API

Las API se han utilizado principalmente para el backend de las aplicaciones empresariales durante muchos años, en concreto, para la comunicación máquina a máquina. En la actualidad, están por todas partes y permiten el funcionamiento de la mayoría de las aplicaciones web y móviles que usamos a diario tanto para el trabajo como por entretenimiento. Constituyen el núcleo de los negocios, impulsan las plataformas digitales modernas y hacen posible la transformación digital.



Barracuda

Las organizaciones se han volcado en el desarrollo de aplicaciones orientado a las API, ya que este método les permite innovar y comercializar sus productos y servicios con rapidez. Combinadas con la metodología ágil y las prácticas DevOps, las API ofrecen entregas rápidas y, a los desarrolladores, la capacidad de compilar y publicar con gran velocidad nuevas funciones para las aplicaciones web y móviles. A medida que se extiende su uso, las API se están convirtiendo en la base de servicios esenciales para las aplicaciones, y, en consecuencia, el acceso que tienen a datos críticos se ha incrementado de forma exponencial.

Su crecimiento y el acceso directo a datos clave que representan, han colocado a las API en el centro de todas las dianas de los atacantes. Las API se desarrollan con el objetivo de automatizar los procesos, de modo que identificar y explotar las menos seguras resulta muy rentable para los atacantes. Con ataques automatizados, los ciberdelincuentes extraen los datos de forma más rápida y sencilla que con cualquier otra aplicación. En las aplicaciones basadas en API, la lógica empresarial se codifica en la aplicación en sí, a diferencia de lo que ocurría con las aplicaciones tradicionales, en las que la lógica quedaba ocultaba en el servidor de backend. Debido a esto, un atacante puede rastrear el tráfico de las aplicaciones para identificar los extremos de las API y lanzarles ataques.

En el informe BugCrowd PriorityOne de 2021, se corrobora el hecho de que las API se han convertido en el nuevo gran objetivo de los atacantes. El informe revela que las vulnerabilidades de las API se han duplicado en tan solo un año; y se espera que sigan creciendo a este vertiginoso ritmo hasta convertirse en uno de los principales vectores de las violaciones de aplicaciones de los próximos años.

Las vulnerabilidades de las API se han

duplicado

en un año

Barracuda

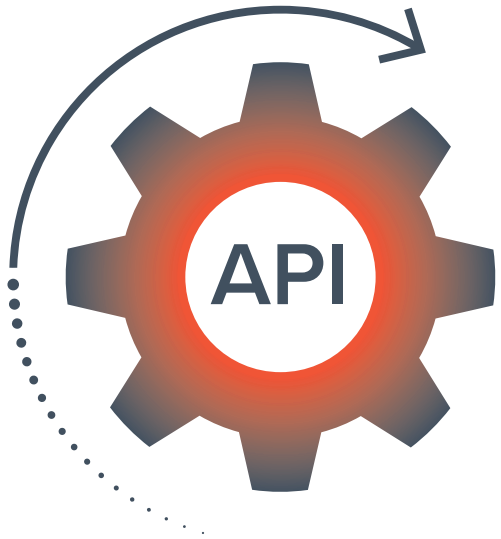
Ejemplo: Exposición de calificaciones crediticias por la API de Experian

Un investigador descubrió recientemente una gran vulnerabilidad en una API mientras buscaba préstamos estudiantiles en línea. Al acceder al sitio web de un prestamista, se le ofreció la posibilidad de comprobar si reunía los requisitos para obtener un préstamo introduciendo su nombre, dirección y fecha de nacimiento. Su naturaleza investigadora lo llevó a consultar el código que se estaba ejecutando tras esta búsqueda y descubrió que se trataba de una llamada a la API de Experian. La API en uso permitía a los prestamistas enviar consultas automatizadas y obtener las calificaciones crediticias de FICO de la oficina de crédito.

El investigador comprobó que se podía acceder directamente a la API de Experian sin necesidad de usar ningún tipo de seguridad de aplicaciones y que, introduciendo ceros en el campo de fecha de nacimiento, se podía obtener la calificación crediticia de cualquier persona. A continuación, desarrolló una práctica herramienta para automatizar las consultas: además de las calificaciones crediticias, la API mostró cuatro “factores de riesgo” que podrían explicar la obtención de una calificación u otra.

Cuando se comunicó el problema a Experian, esta solo tuvo que eliminar el acceso a la API de este extremo.

La herramienta creada por el investigador evidenció lo peligrosa que era esta exposición. En este caso, se trataba de un investigador que informó de lo ocurrido para que Experian corrigiera el problema, pero, en caso de que un autor malicioso hubiera hallado este extremo de la API, podría haberlo usado para recopilar calificaciones crediticias de toda persona con nombre y dirección públicos, y, posiblemente, ocasionar un gran daño. Se desconoce si la llamada a la API tuvo como consecuencia una verificación de crédito más o menos exhaustiva y el efecto de la visualización de la calificación en la puntuación crediticia de cada persona.



Ejemplo: Ataque de fuerza bruta a las contraseñas de las reuniones privadas en Zoom

Las reuniones de Zoom se protegían de forma predeterminada con una contraseña numérica de seis dígitos, de modo que a cada una de ellas le correspondía una contraseña de entre un millón de posibilidades. Un investigador descubrió que estas contraseñas estaban recibiendo ataques de fuerza bruta, lo que, a su vez, provocaba ataques de bombing y otros tipos similares a Zoom.

Cuando Zoom contaba con contraseñas numéricas, se accedía a las reuniones a través de un enlace, que redirigía a una página web en la que se solicitaba la contraseña. Cuando se rellenaban los campos pertinentes y se pulsaba la tecla “Entrar”, se podían observar las interacciones de la API de backend y detectar la vulnerabilidad.

Lo más preocupante que se descubrió es que este proceso no contaba con un límite de frecuencia, es decir, el investigador pudo probar distintas contraseñas de forma ininterrumpida y, tras 43 164 intentos, que realizó en unos 29 minutos, dio con la correcta. Esto equivale a una frecuencia de unas 25 contraseñas por segundo. Además, si en un ataque se utilizan varias máquinas en paralelo, la contraseña puede descifrarse en muy poco tiempo.

Este hackeo tuvo enormes implicaciones. Dado el elevado número de importantes organismos gubernamentales y organizaciones similares que emplean Zoom, este problema podría haber causado graves daños si, por ejemplo, algunos autores maliciosos se hubieran colado en las reuniones para espiarlas. El investigador hizo llegar esta información a Zoom, que implementó distintos cambios para solucionar el asunto.

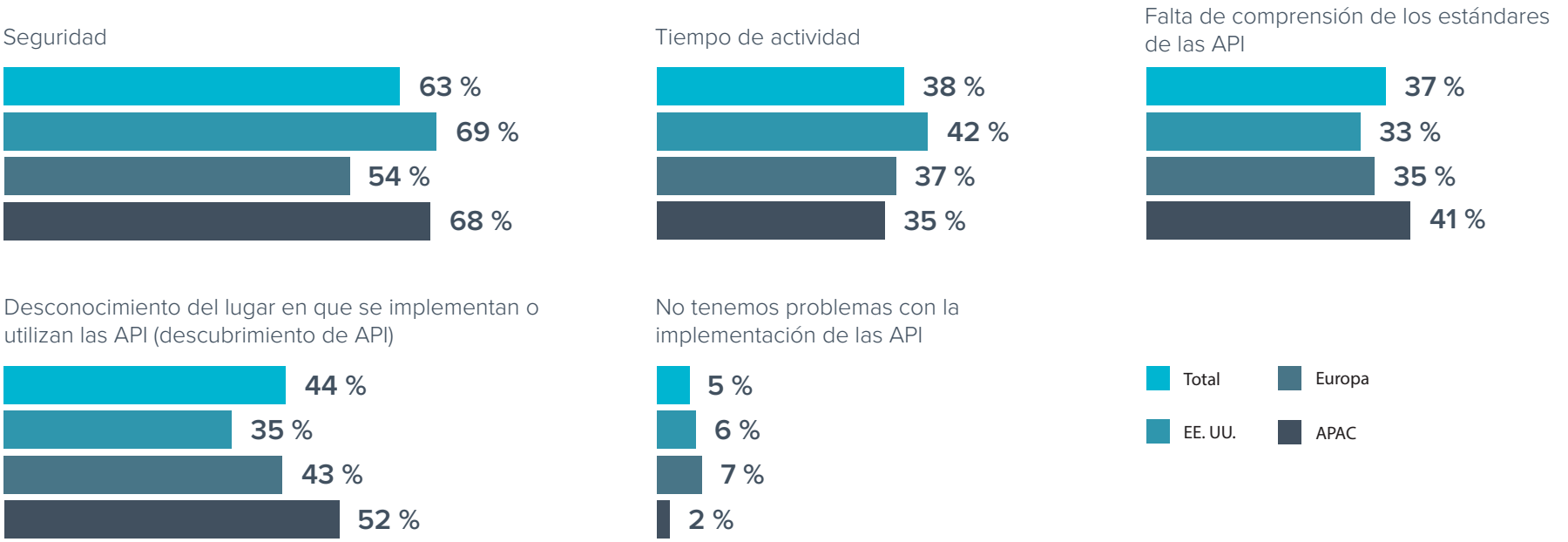
Además de la falta de límite de frecuencia, se descubrió otra gran carencia: la falta de un registro y una supervisión adecuados, que podrían haber alertado fácilmente al equipo de Zoom de estos intentos.

Opinión de los profesionales de la seguridad de aplicaciones

Dado el enorme impacto que puede tener la violación de una API, no es de extrañar que la seguridad de las API sea una de las principales preocupaciones de los encargados de la defensa. En nuestra reciente encuesta realizada a profesionales de la seguridad de las aplicaciones, les preguntamos por las principales dificultades a las que se estaban enfrentando a la hora de implementar API, y la seguridad fue la más repetida. El Open Web Application Security Project (OWASP) lo corrobora en API Security Top 10, que incluye una lista de las vulnerabilidades y los riesgos de seguridad específicos de las API.

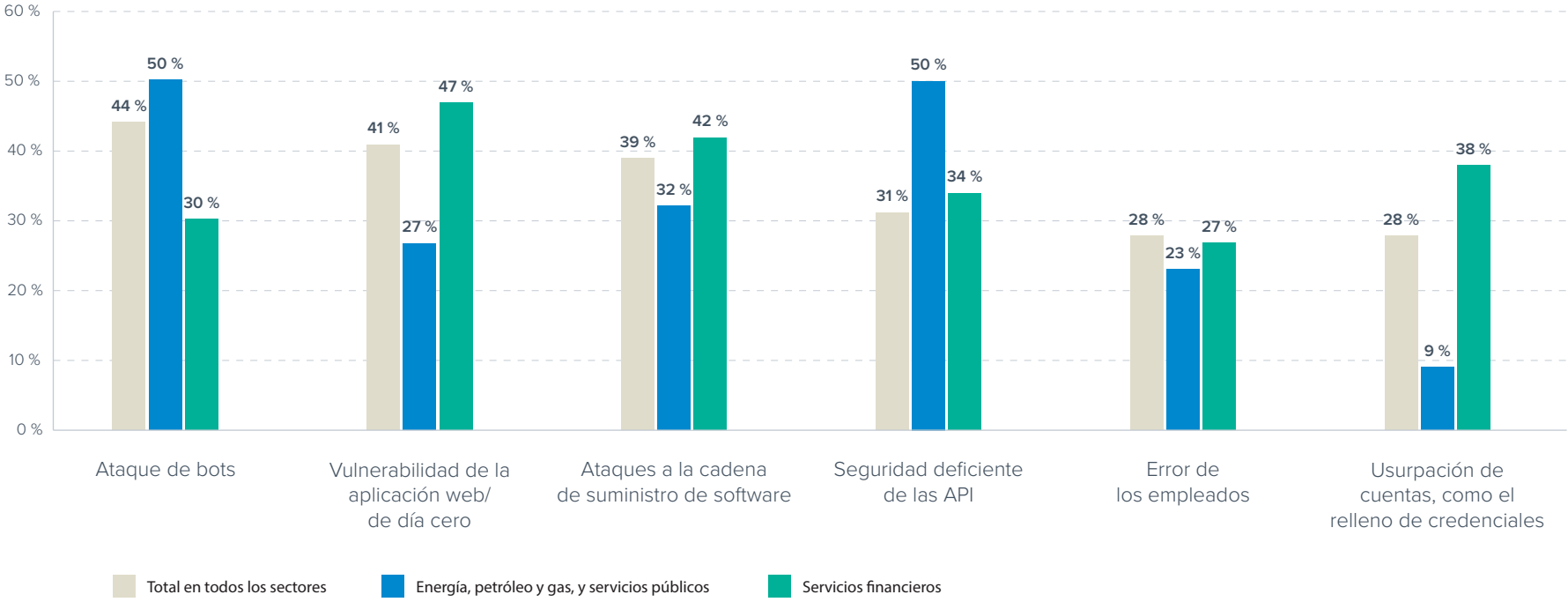
¿Cuáles son los principales problemas que experimenta su organización a la hora de implementar API?

(n=728)



¿Cuál de los siguientes factores ha contribuido a que se produzca una violación de la seguridad de su organización, mediante el aprovechamiento de la vulnerabilidad de una de sus aplicaciones, en los últimos 12 meses?

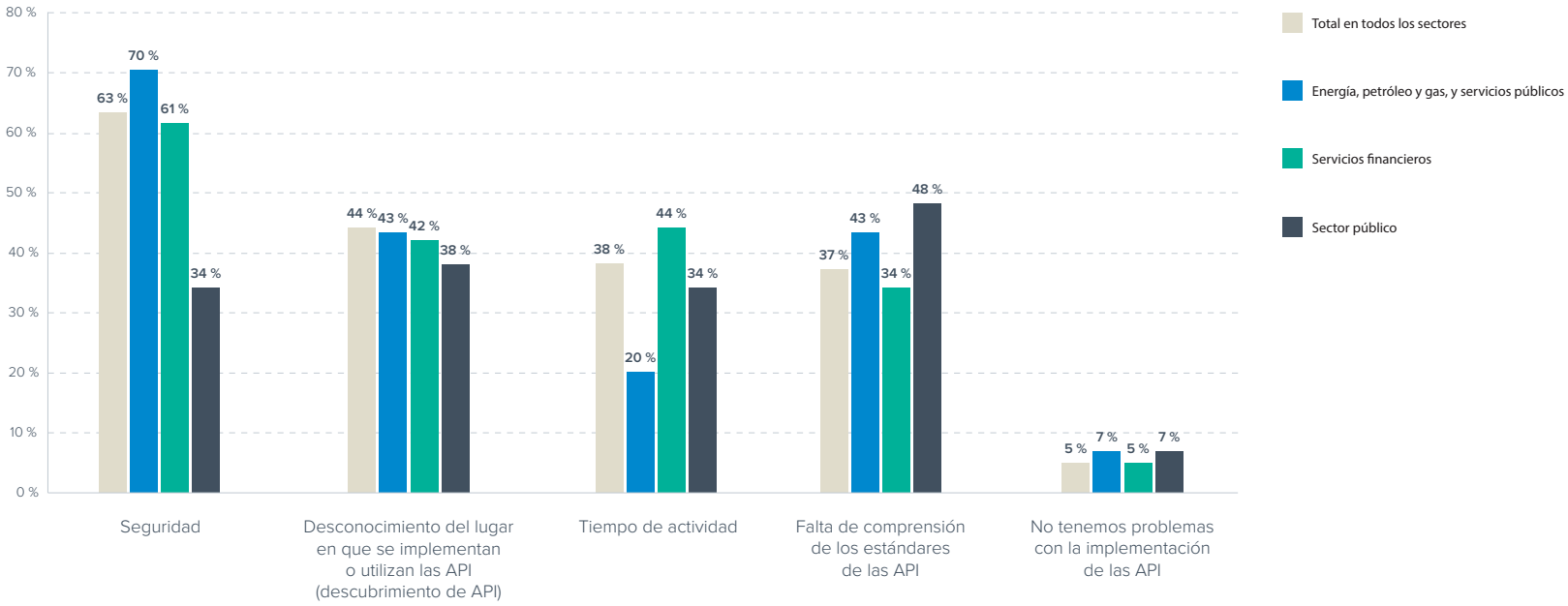
(n=541)



Según los resultados de la encuesta, los sectores de la energía, el petróleo, el gas y los servicios públicos eran los más propensos a sufrir violaciones debido a una vulnerabilidad de la API. Si bien estos sectores suelen ser noticia por los ataques de IdC y ransomware dirigidos, sus API, muchas de las cuales están orientadas al público, también se encuentran bajo una importante amenazada de ataque. Los encuestados pertenecientes al sector de los servicios financieros, en el que las API son la base de las transacciones automatizadas, también señalaron las vulnerabilidades de las API como principal motivo de violación.

¿Cuáles son los principales problemas que experimenta su organización a la hora de implementar API?

(n=728)

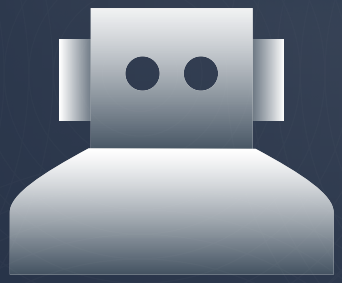


El sector público es el que menos probabilidades tiene de experimentar problemas a la hora de implementar API, de acuerdo con sus respuestas. Lo curioso es que su principal problema es la "falta de comprensión de los estándares de las API", mientras que la seguridad de las API ocupa la tercera posición, con un porcentaje muy inferior. En cambio, la práctica totalidad del resto de los sectores cita la seguridad de las API como su máxima prioridad. En concreto, los sectores de la energía, el petróleo, el gas y los servicios públicos encabezan la lista de los sectores con mayor preocupación en este sentido.

Como cabría esperar, los encuestados pertenecientes a organizaciones financieras fueron los que se mostraron más preocupados por el tiempo de actividad. En cuanto a conformidad con los estándares, los profesionales de los sectores de la energía, el petróleo, el gas y los servicios públicos fueron quienes más la desconsideraron, lo que, en cierto modo, es motivo de alarma, ya que la conformidad con los estándares en el desarrollo de las API garantiza una mayor seguridad.

B de protección frente a los bots

En los últimos años, el tráfico de bots automatizados se ha incrementado muy rápido. Los bots, que antes solían utilizarse principalmente en los motores de búsqueda, ahora tienen una amplia variedad de usos, tanto bien como malintencionados. La mayoría de los bots benignos son rastreadores de motores de búsqueda, bots de redes sociales, rastreadores de agregadores o bots de monitorización, entre otros. Estos bots obedecen las reglas del propietario del sitio web especificadas en el archivo robots.txt, publican métodos para validar su identidad, y trabajan de forma que no saturen los sitios web y las aplicaciones que visitan.

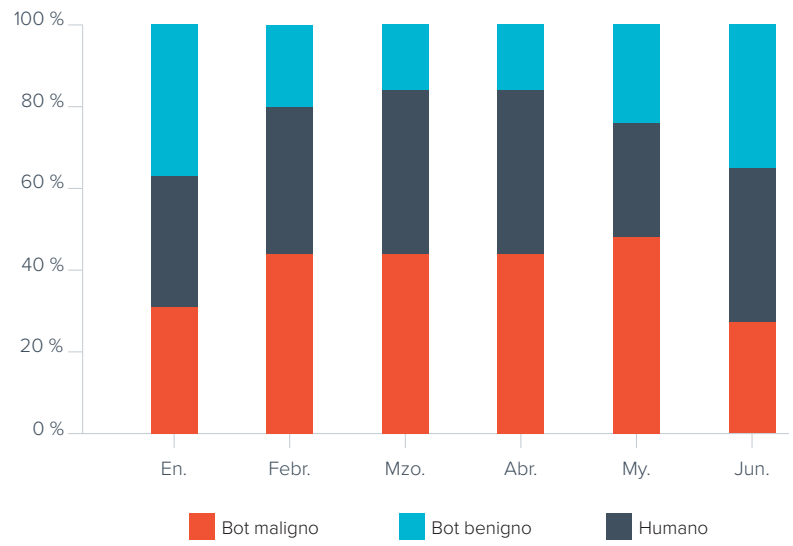


Barracuda

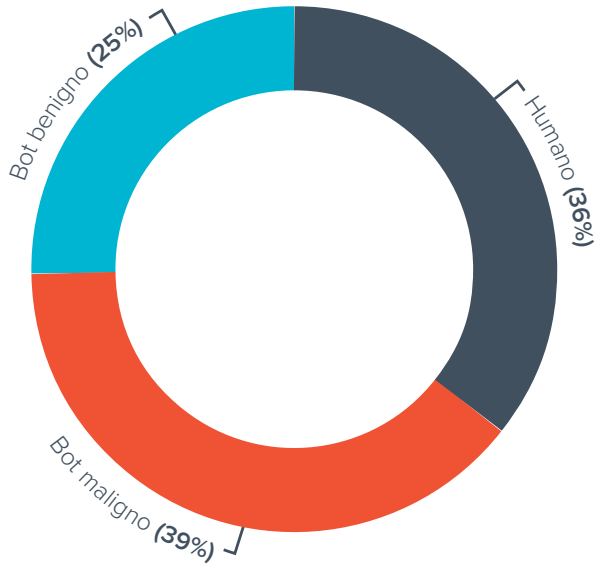
Los bots malignos se desarrollan para llevar a cabo distintas actividades malintencionadas. Pueden ser desde rastreadores básicos que intentan obtener determinados datos de una aplicación (y que se bloquean fácilmente), hasta bots persistentes avanzados que se comportan casi como seres humanos y tratan de evitar ser descubiertos en la medida de lo posible. Estos bots llevan a cabo ataques como el raspado de precios y web, el secuestro de inventarios, la usurpación de cuentas, la denegación de servicios distribuidos (DDoS) y muchos otros tipos. En la actualidad, los bots malignos constituyen una parte significativa del tráfico de los sitios web, por lo que su detección y bloqueo son críticas para las empresas.

El tráfico automatizado representa casi dos tercios del tráfico de Internet, según la medición realizada con la tecnología de Barracuda durante los primeros seis meses de 2021. Alrededor de un 25 % de este tráfico se corresponde con bots benignos, como rastreadores de motores de búsqueda, y bots de redes sociales y de monitorización.

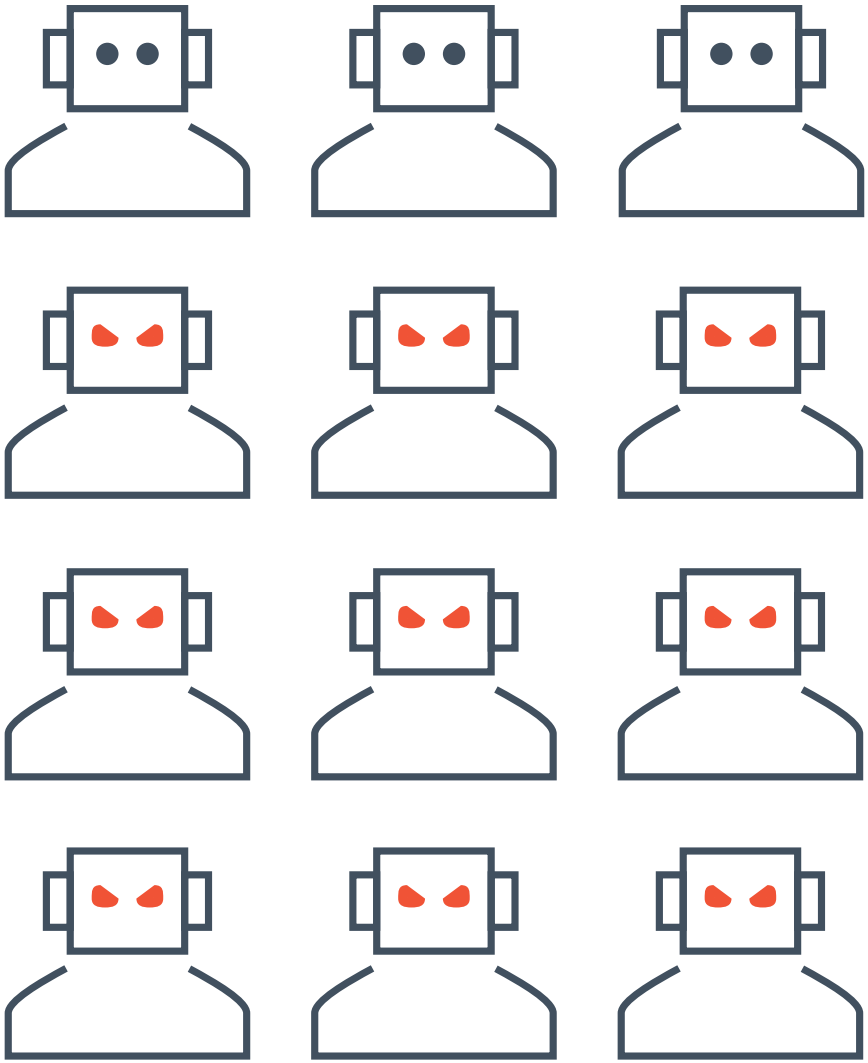
Distribución por mes



Distribución del tráfico: bots vs. humanos (de enero a junio de 2021)



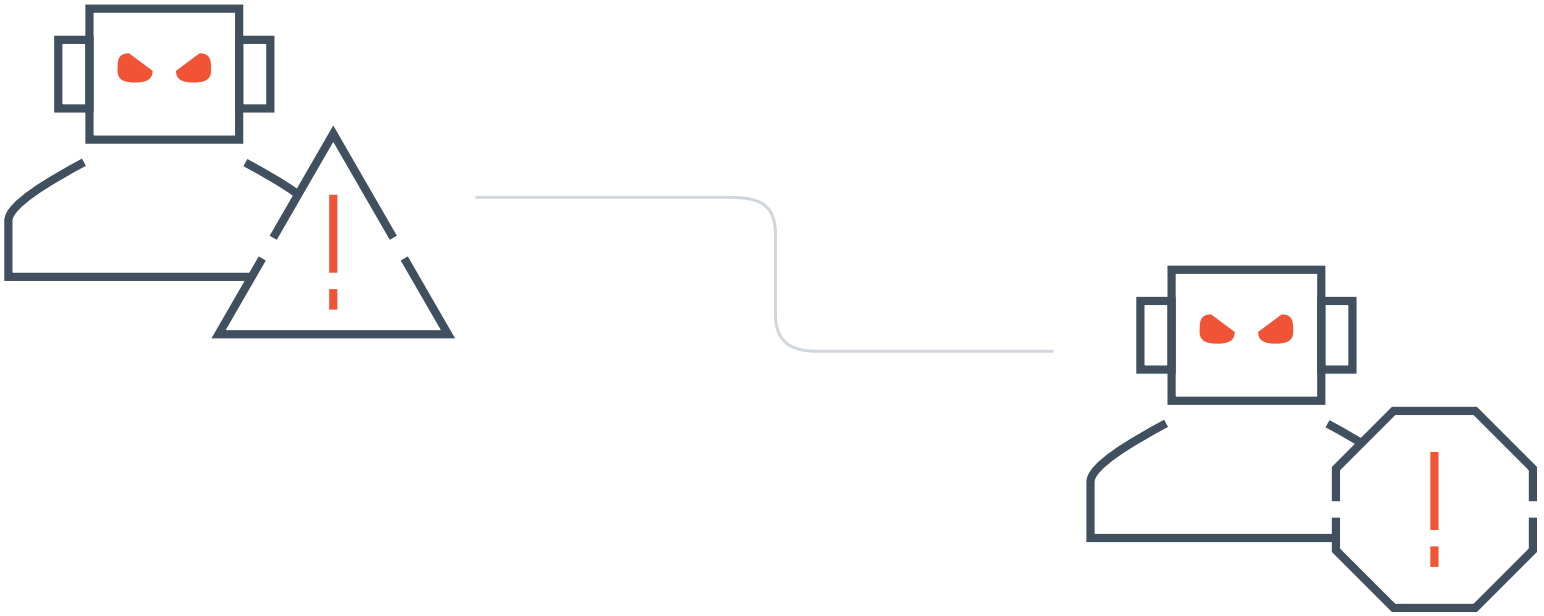
Hoy en día, los bots son muy sofisticados y pueden tener un comportamiento casi humano, que les permite burlar muchas defensas. Las defensas estándares que se emplean para detenerlos, principalmente reCAPTCHA de Google, no suele suponer un gran problema para ellos. De hecho, los bots resuelven los CATPCHAs de imágenes más fácilmente que los humanos. Se ha creado todo un ecosistema en torno a los bots: desde las personas que diseñan estos bots inteligentes, hasta los servicios que ofrecen cuentas de Google con “gran reputación” para eludir los CAPTCHA, pasando por los servicios que ofrecen direcciones IP residenciales (o Resis), a fin de evitar el bloqueo en función de la reputación de la IP, y los servicios de depósitos que evitan que los compradores de bots sean víctimas de estafas. Cada vez más personas recurren a los bots para ganar dinero rápidamente, como en el caso de especulación de la videoconsola PlayStation 5 de diciembre de 2020, por lo que los bots se están convirtiendo en algo muy habitual y en un gran problema.



Ejemplo: Raspado de los precios de una tienda de comercio electrónico de Europa del Este

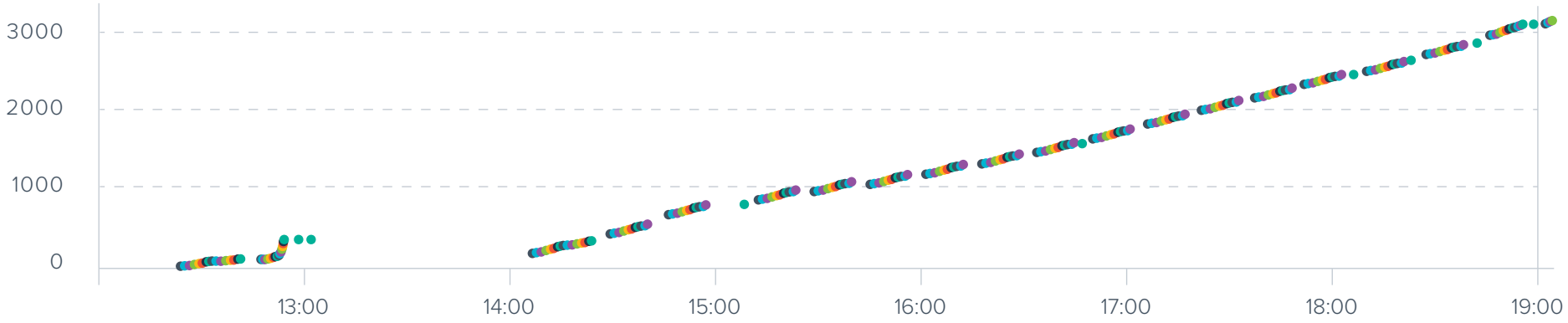
Barracuda detectó y detuvo un intento de raspado de precios de una tienda de comercio electrónico de Europa del Este. La tienda en cuestión estaba ofreciendo un descuento en los productos de Apple, cuando se observaron en el tráfico algunos patrones de comportamiento sospechosos. Este anormal tráfico procedía de clientes con navegadores estándares, a través de numerosas direcciones IP residenciales locales. No obstante, estas direcciones IP locales pertenecían a proveedores de alojamiento de VPS y cada cliente solo estaba accediendo a un conjunto determinado de páginas.

Se sorprendió a los atacantes sacando provecho de esta correlación y el intento de raspado de precios se detuvo con éxito.



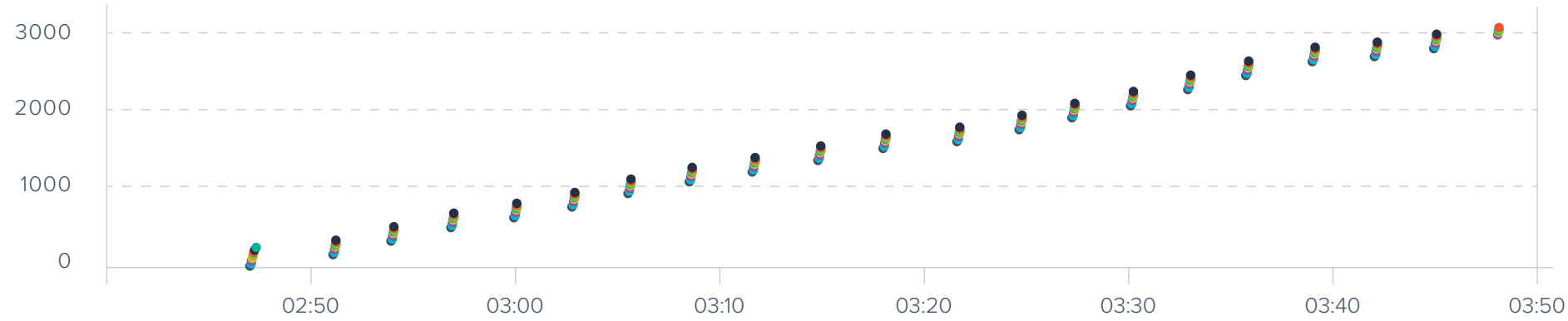
Barracuda

Patrón de repetición de un bot de raspado de precios



Una hora después de que se frenara la primera oleada, los bots accedieron varias veces al mismo conjunto de URL de productos.

Patrones de cambio de bots para intentar evitar ser detectados

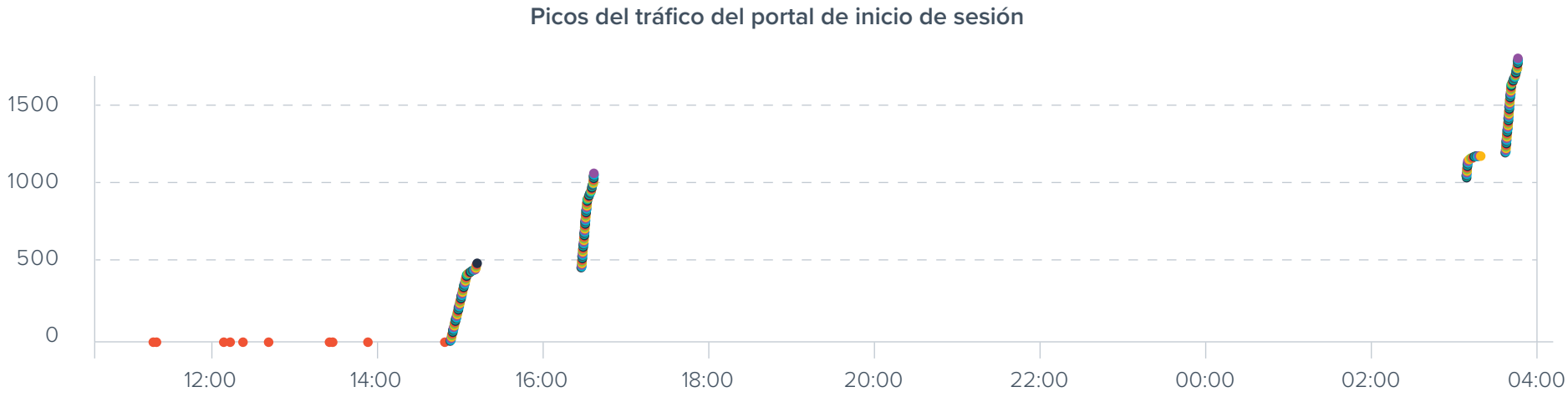


Los bots intentaron acceder varias veces a un conjunto más pequeño de páginas de productos siguiendo un patrón de navegación diferente en una hora.

Barracuda.

Ejemplo: Intento de sobrecargar el portal de inicio de sesión de una empresa de fabricación india

Una empresa de fabricación india observó un inusual aumento del tráfico de su portal de inicio de sesión. La mayor parte de este tráfico procedía de redes móviles, lo cual es poco habitual, pero no inesperado en este sitio web. Sin embargo, un análisis más exhaustivo reveló que el tráfico entrante podía partir de un navegador de un ordenador de sobremesa conectado a un punto de acceso que se estuviera haciendo pasar por un dispositivo móvil. Así, se bloquearon correctamente todos los clientes que estaban intentando sobrecargar la página de inicio de sesión y se restableció el tiempo de respuesta de la página.



Los primeros puntos corresponden al bot haciéndose pasar por humano y ampliando el acceso. Después, aparecen grupos de puntos: cada punto representa a cada cliente diferente que intentó acceder a la página de inicio de sesión.

Barracuda.

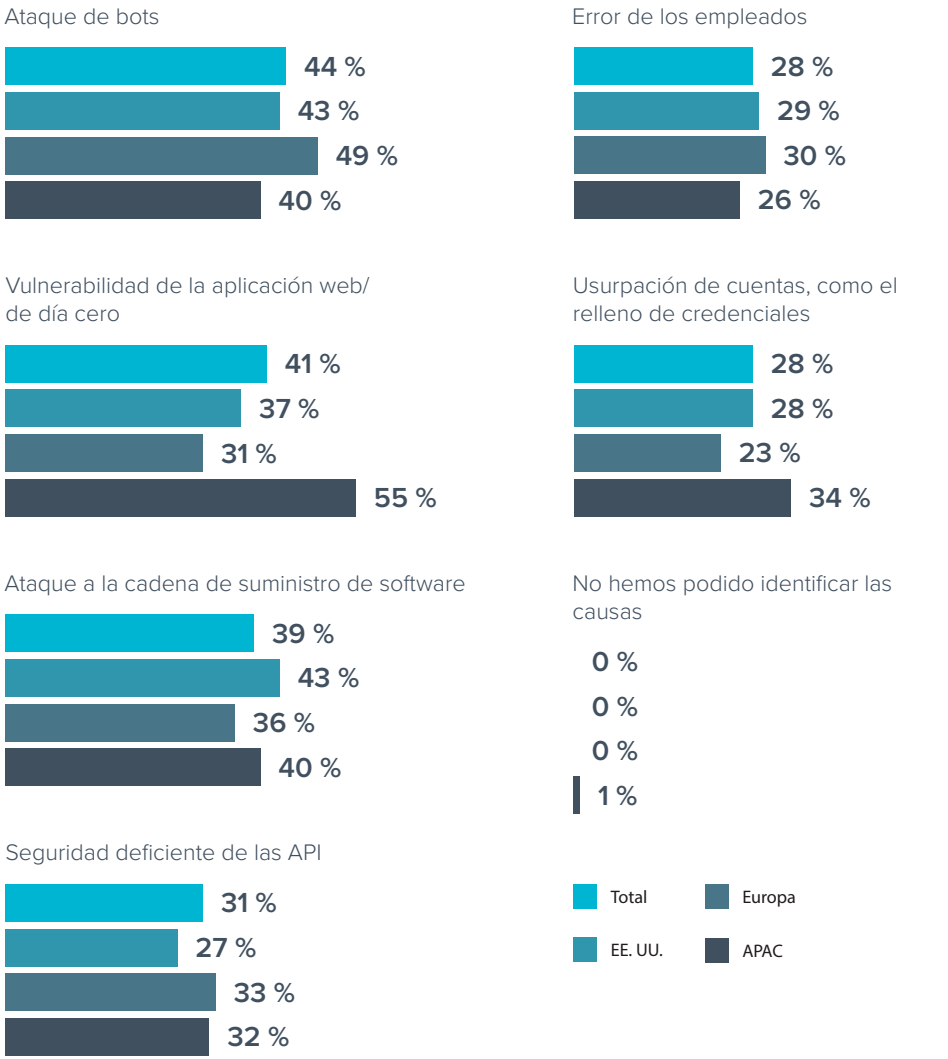
Opinión de los profesionales de la seguridad de aplicaciones

En los últimos años, los ataques de bots han aumentado rápidamente, lo que ha traído consigo algunos peligros significativos. Hace dos años, las mayores amenazas que planteaban los bots eran los ataques de usurpación de cuentas y relleno de credenciales; se publicaban constantemente ataques de este tipo, así como declaraciones públicas de "volcados de credenciales" por parte de sitios como LinkedIn.

Según la reciente encuesta que hemos realizado a profesionales de la seguridad de las aplicaciones, los ataques de bots eran el factor que más contribuía a que se produjera violaciones de la seguridad como consecuencia directa de la vulneración de una aplicación en los últimos 12 meses.

¿Cuál de los siguientes factores ha contribuido a que se produzca una violación de la seguridad de su organización, mediante el aprovechamiento de la vulnerabilidad de una de sus aplicaciones, en los últimos 12 meses?

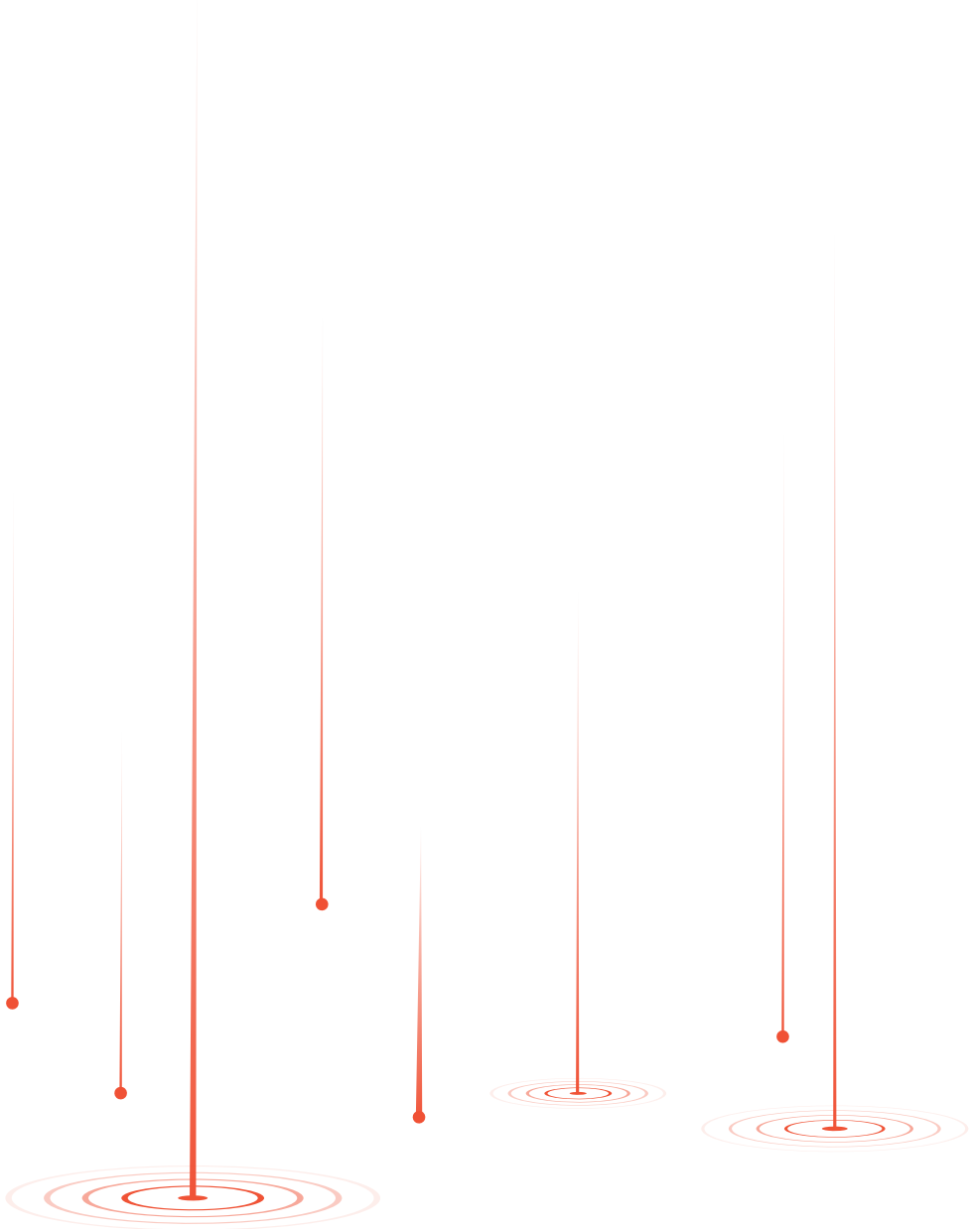
(n=541)



Debido al amplio abanico de ataques de bots que se lanzan a las aplicaciones, su detención puede ser todo un rompecabezas.

Dada la variedad de formas que puede adoptar este vector de ataque, no es de extrañar que tantas organizaciones tengan problemas para defender sus aplicaciones de los bots. Aunque el daño que suele producir el spam mediante bots sea el mero fastidio, a menudo se utiliza como cortina de humo para ocultar un ataque más malicioso, por lo que no debe ignorarse. En función de su frecuencia y autenticidad, el spam mediante bots puede convertirse en un huesecillo duro de roer y pasar de ser un simple incordio a generar problemas operativos de mayor importancia muy fácilmente.

La suplantación de navegadores y aplicaciones por bots también suponen problemas significativos. Pueden ser muy simples o complejos, desde el intento de un usuario de ocultar su navegador hasta bots que ejecutan versiones afectadas de las aplicaciones en granjas de clic para el fraude publicitario u otros fines maliciosos.

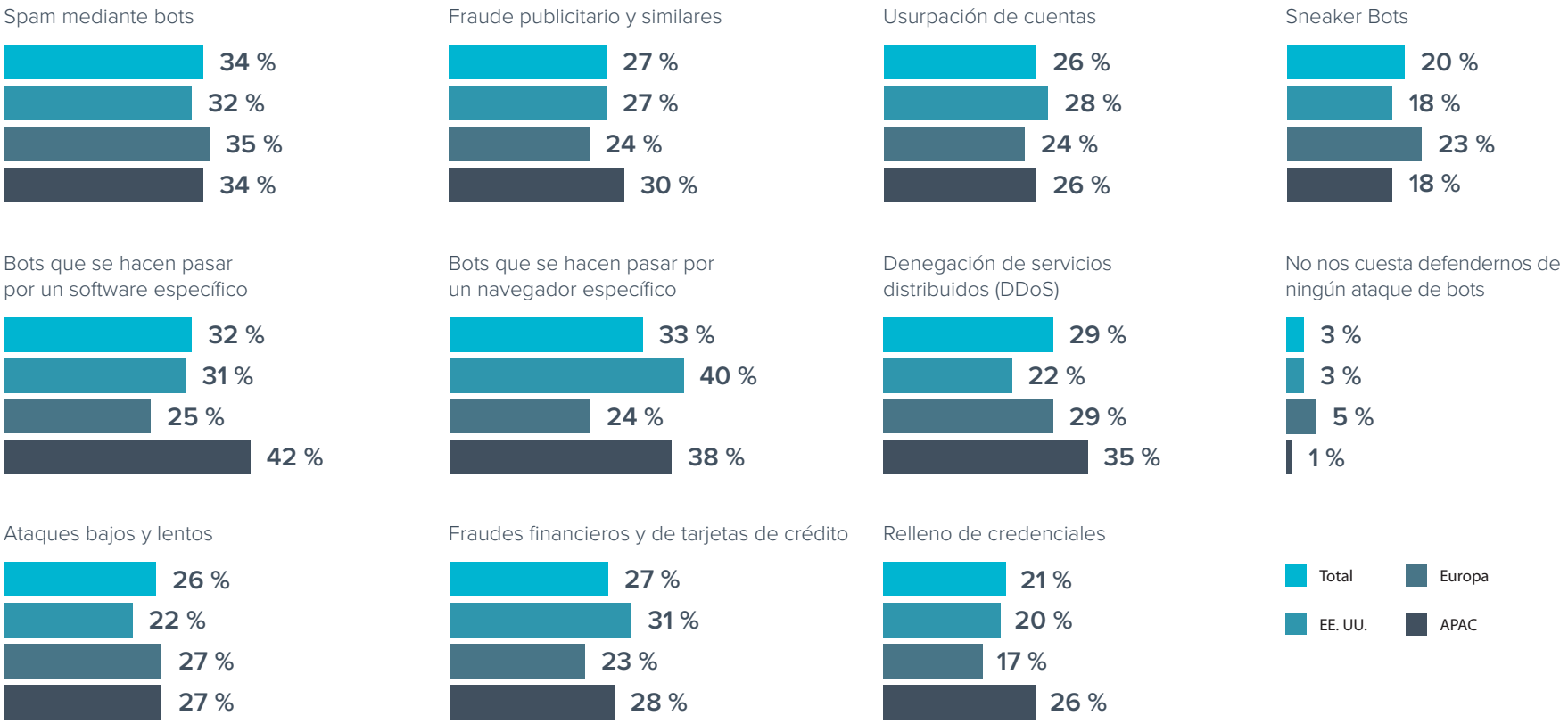


Barracuda

La combinación de estos tipos de bots aumenta las probabilidades de éxito. Los ataques de bots bajos y lentos de varios vectores son la base del problema y lo más probable es que contribuyeran a que se produjeran las violaciones de seguridad del año pasado.

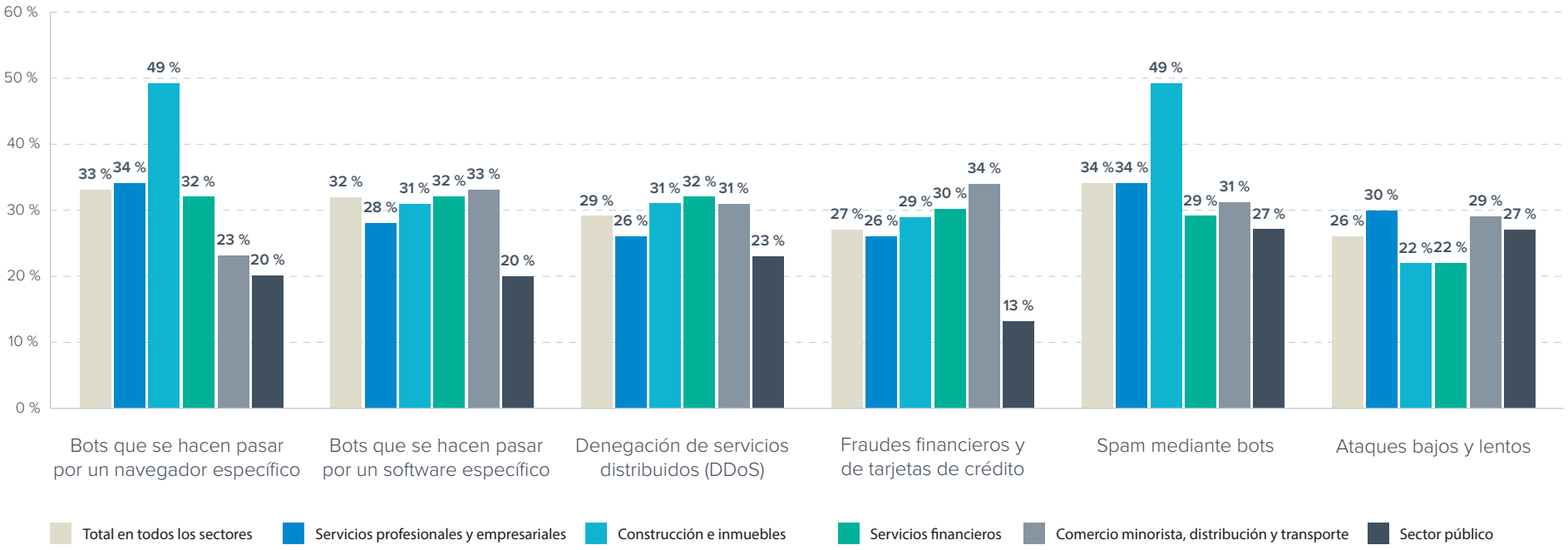
De los distintos tipos de ataques de bots lanzados a las aplicaciones, ¿de cuáles le cuesta más a su organización defenderse?

(n=750)



De los siguientes tipos de ataques de bots lanzados a las aplicaciones de su organización, ¿de cuáles le cuesta más defenderse?

(n=750)



Los tres tipos de ataques de bots de los que más les cuesta defenderse a los encuestados del sector de servicios financieros son la denegación de servicios distribuidos, los bots que se hacen pasar por un software específico y los bots que se hacen pasar por un navegador específico. Estos tipos de usurpaciones representan un gran problema para las aplicaciones financieras: los atacantes utilizan versiones crackeadas para llevar a cabo acciones malintencionadas contra estas organizaciones. La denegación de servicios distribuidos implica pérdidas financieras significativas, ya que estos servicios no están disponibles.

También resulta interesante el hecho de que los fraudes financieros y de tarjetas de crédito ocupen la segunda posición de la lista, puesto que cabría esperar encontrarlos en lo más alto. Esto pone de manifiesto la gran importancia que tiene el acceso mediante navegadores o aplicaciones en las organizaciones financieras, que seguirá aumentando.

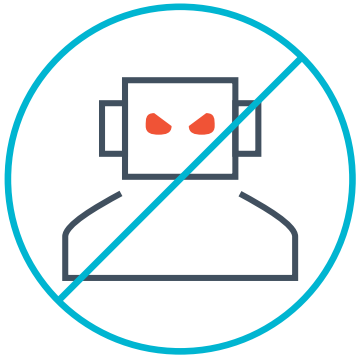
En general, los bots que se hacen pasar por un software o un navegador específico representan uno de los cinco problemas principales de la mayoría de los sectores. Otro dato interesante es la gran preocupación que sienten el sector público y el de la construcción y los inmuebles ante el spam mediante bots, lo que sugiere que los sitios web inmobiliarios deben estar sufriendo mucho spam en sus anuncios. El spam en el sector público también supone un gran problema; por ejemplo, hace unos años, la cantidad de spam entrante en los debates sobre la neutralidad de la red de la FCC supusieron un motivo de gran preocupación.

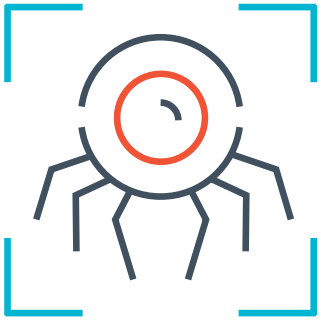
Los ataques de bots bajos y lentos preocupan más al sector público, al comercio minorista, y a los servicios profesionales y empresariales. En las organizaciones públicas, suele haber muchos archivos para descargar sin puertas de enlace, por lo que se convierten en el objetivo de los ciberdelincuentes que intentan llevar a cabo ataques de denegación de servicios distribuidos contra las aplicaciones. El comercio minorista también tiene mucho que perder ante los bots bajos y lentos que intentan acometer distintos ataques, como la usurpación de cuentas, el raspado de precios y la especulación, entre otros muchos.

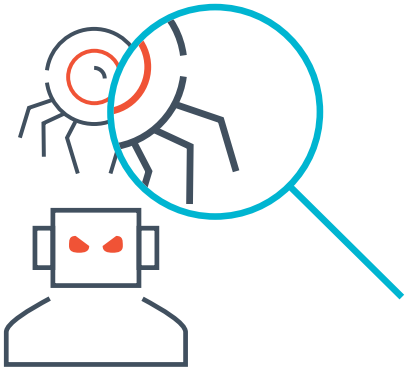
Es fundamental que los proveedores que ayuden a las organizaciones a defenderse de los ataques de bots les ofrezcan funciones de prevención, detección e identificación de bots.

Es fundamental que los proveedores que ayuden a las organizaciones a defenderse de los ataques de bots les ofrezcan funciones de prevención, detección e identificación de bots.

Las organizaciones necesitan implementar mejoras en defensa frente a este vector de ataque, independientemente de si su principal problema viene del spam mediante bots, los bots fraudulentos o los bots que suplantan un software o navegador. Al fin y al cabo, los bots fueron el vector que más contribuyó a que se produjeran violaciones de seguridad de las aplicaciones en el último año. Según los encuestados, a la hora de decantarse por una solución de seguridad para defenderse de los bots, las tres funciones principales que tendrían en cuenta son la prevención, la detección y la identificación de bots.



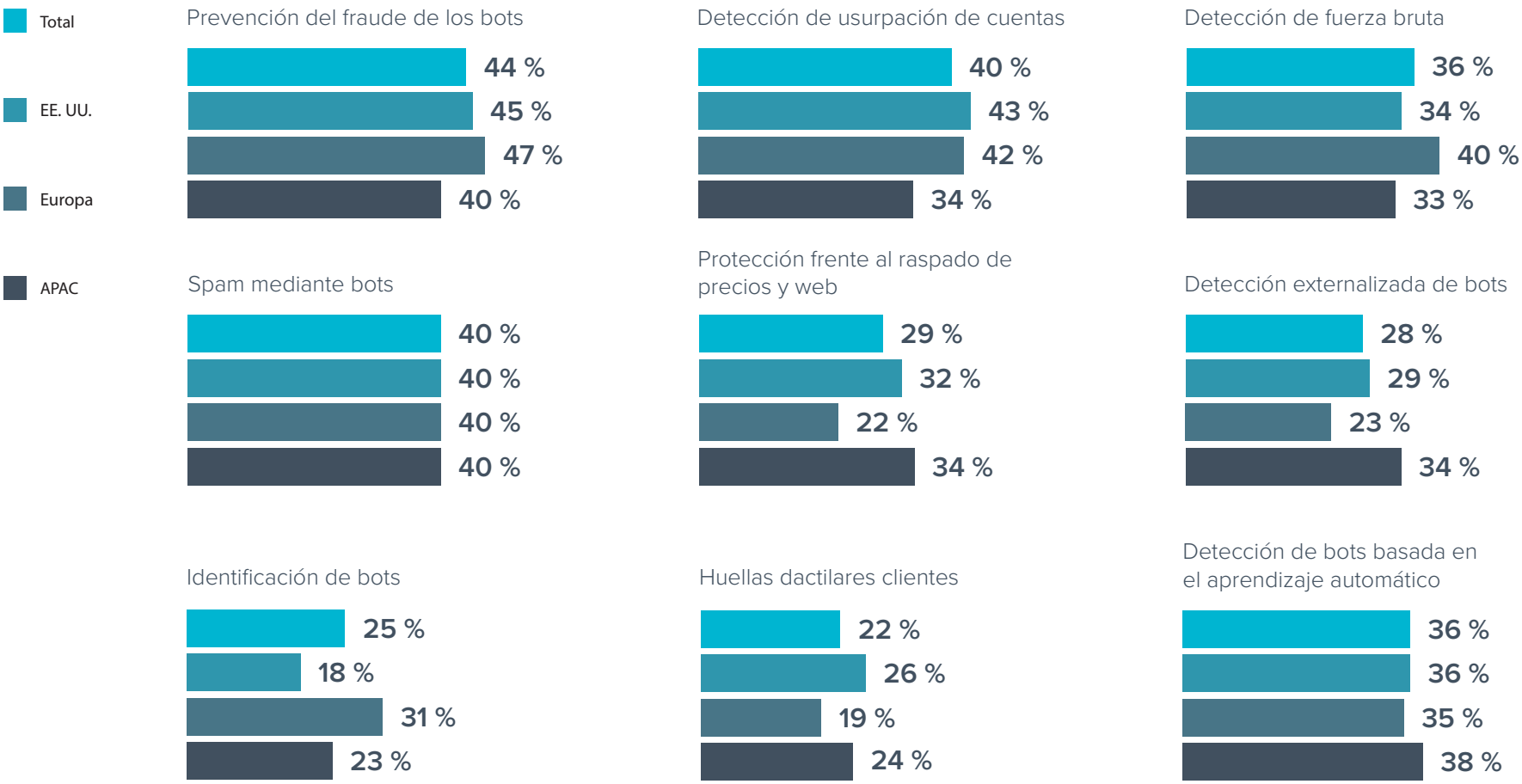




Estas funciones son fundamentales para defenderse de la mayoría de los tipos de ataques, pero los proveedores deben proporcionarlas en una única solución a fin de mejorar considerablemente las capacidades de protección contra bots de la mayoría de las organizaciones.

A la hora de decantarse por una solución de seguridad para defender las aplicaciones de los posibles ataques, ¿qué funciones resultan más importantes para su organización?

(n=750)



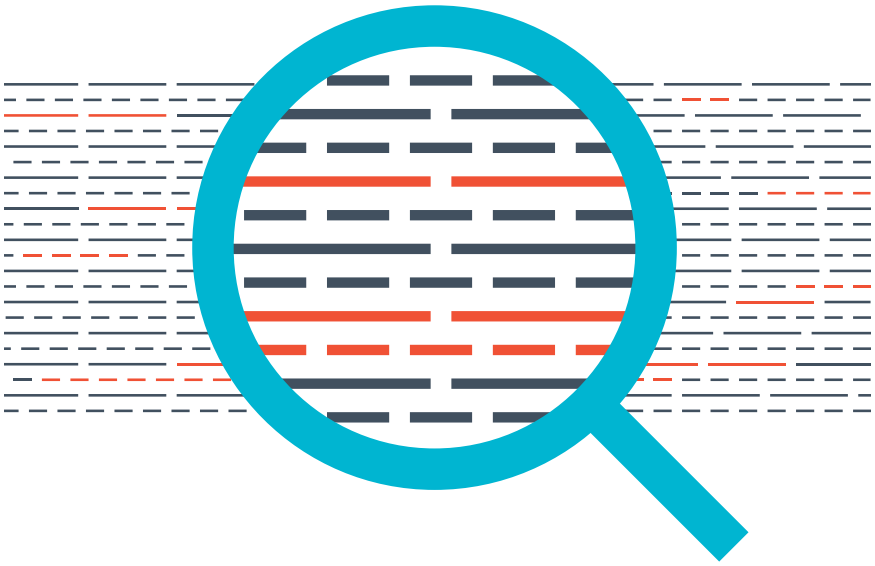
C de protección del lado del cliente

A lo largo de los años, han emergido una amplia variedad de novedosas vulnerabilidades específicas de la web, como el clickjacking, o ataque de compensación de UI, y las secuencias de comandos en sitios cruzados. Muchas de ellas se ponen de manifiesto en el lado del cliente y, por desgracia, las vulnerabilidades que surgieron en el lado del cliente hace más de una década, siguen presentes.

Detectar y detener los ataques del lado del cliente, también conocidos como ataques a la cadena de suministro o Magecart (en referencia a la aplicación de compra Magento, que recibió el primer ataque de este tipo) resulta muy complicado.

Barracuda

Desde los comienzos de la web, a finales de los ochenta, las aplicaciones no han dejado de evolucionar para satisfacer nuestro insaciable apetito de Internet. Este cambio no solo ha ocurrido en el lado del servidor, sino también en el del cliente, es decir, en el navegador. Al igual que el contenido dinámico sustituyó al estático, las aplicaciones de una página sustituyeron a la simple representación de JavaScript con una experiencia más acorde a los desplazamientos con el dedo de los dispositivos móviles y las tablets. Una parte cada vez mayor de la lógica de las aplicaciones se traslada al lado del cliente, por lo que los atacantes han dirigido su atención también a este lado. La mayoría de esta lógica se implementa con código abierto o de terceros, un proceso en el que la seguridad queda en segundo plano.



Los desarrolladores recurren al código de terceros porque la web moderna no podría construirse sin él. Las páginas web modernas contienen docenas o incluso cientos de scripts externos de terceros o cuartos. Se pueden utilizar herramientas como webpagetest.org para consultar el sorprendente número de scripts de terceros incluidos en una página web determinada. Este enfoque se acepta en el campo del desarrollo web porque la alternativa es inconcebible: reinventar miles de líneas de código. El problema reside en la confianza: un script que es inofensivo hoy puede hackearse mañana. Los atacantes tienen como objetivo las fuentes que alojan este código de terceros, ya que su hackeo permitirá que cada aplicación que utilice ese código pase a ser una víctima.

Como lo que se modifica de forma malintencionada es el código de terceros, la mayoría de los propietarios de las aplicaciones no se dan cuenta de que los scripts se han visto vulnerado hasta mucho más tarde. Los propios scripts se cargan desde otras fuentes, como redes de distribución de contenido y repositorios de código, y, por lo general, no se envían de forma directa al navegador desde el sitio web, por lo que detectarlos y detenerlos resulta muy complicado con las herramientas y prácticas de las que disponemos actualmente.

Ejemplo: Ataque a la cadena de suministro de British Airways

En 2018, un ataque a una cadena de suministro supuso la filtración de los datos de entre 380 000 y 500 000 clientes de British Airways. La violación conllevó la pérdida de información personal y de pago de los afectados.

Esta filtración fue uno de los mayores ataques de Magecart de aquella época. Magecart era un grupo cuya actividad se detectó por primera vez en 2016, cuando se dedicaban a robar datos de tarjetas en línea. Inyectaban scripts que robaban los datos de otros métodos de pago en línea y, después, utilizaban ellos mismos los datos robados o los vendían a otros ciberdelincuentes.

En el caso de British Airways, el grupo Magecart modificó el JavaScript que se utilizaba en las aplicaciones web y móviles de la aerolínea, llamado Modernizr. En concreto, incrustó una pequeña función en el script para que se ejecutara al final de este y recopilara los datos introducidos en el método de pago, que se enviarían a un sitio web de terceros gestionado por el grupo. El resultado fue una extracción masiva de datos y una multa de 20 millones de libras a British Airways, que fue la mayor multa impuesta en Reino Unido en la época (se redujo de los 183,39 millones de libras debido a las repercusiones económicas de la pandemia en los sectores de las aerolíneas y los viajes).

Clientes afectados por las **filtraciones de datos**

380 000 - 500 000

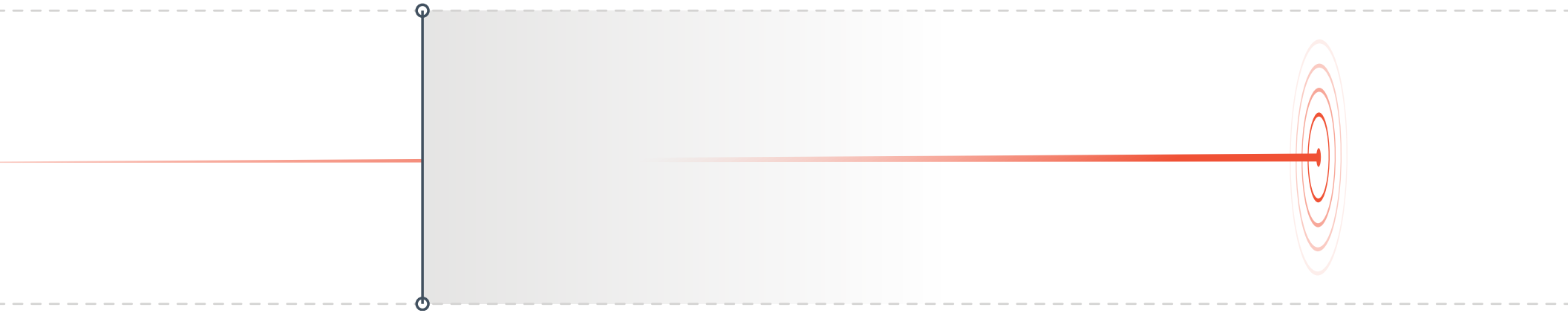
De **multa** a British Airways

20 £ millones

Ejemplo: Advertencia de la existencia de un skimmer en línea por parte de Visa

En septiembre de 2020, Visa publicó una advertencia sobre la existencia de un nuevo skimmer en línea llamado Baka, que estaba llevando a cabo ataques de skimming del lado del cliente. El skimmer disponía de una serie muy interesante de mecanismos para evitar su detección: se cargaba de forma dinámica en la memoria del equipo del cliente en el momento de la ejecución, de modo que los análisis estándares o la inspección de páginas no podían detectarlos. Además, estaba diseñado para ejecutarse solo desde la memoria para no dejar rastro en el almacenamiento del navegador. Los creadores del skimmer se esforzaron mucho para garantizar que estuviera completamente cifrado y que fuera muy difícil de identificar cuando se ejecutara en un sitio web o aplicación.

Cuando se notificó el problema, el skimmer estaba activo en numerosas tiendas en línea y se constató que lo habían diseñado desarrolladores muy cualificados para evitar la detección el mayor tiempo posible.



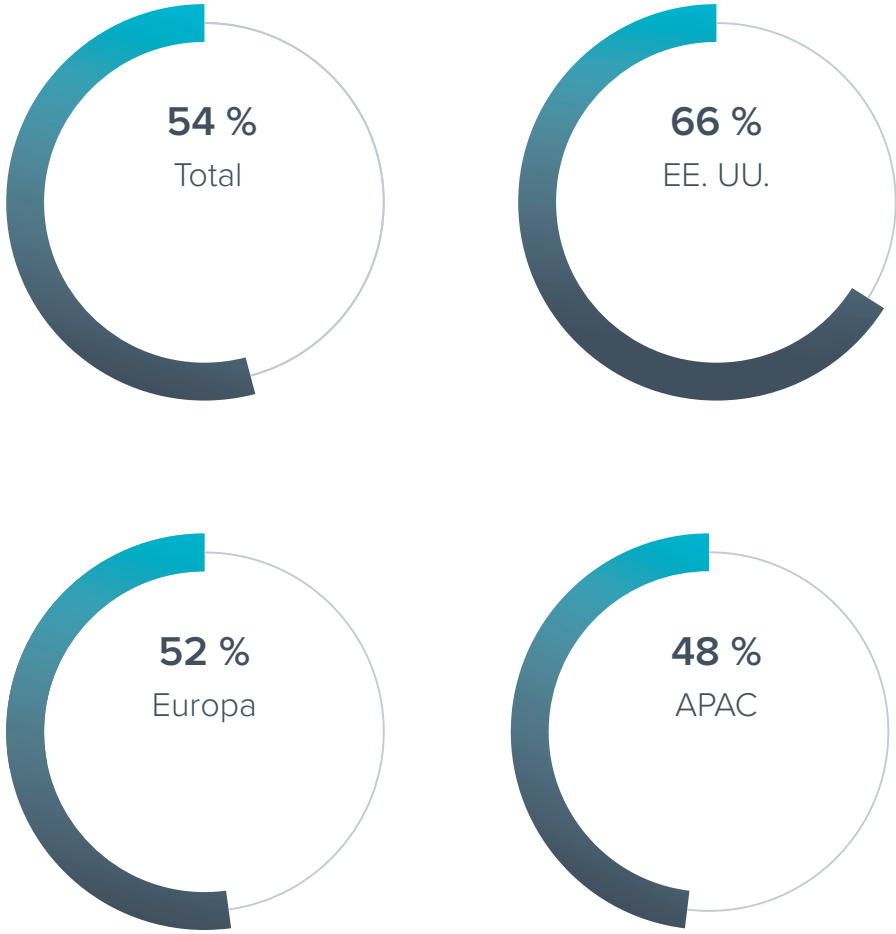
Opinión de los profesionales de la seguridad de aplicaciones

El uso de scripts de terceros en las aplicaciones web es algo bastante generalizado; las organizaciones emplean distintos métodos para enviar los scripts a los navegadores.

De nuevo, la búsqueda de eficiencia en el desarrollo de aplicaciones resulta evidente en las respuestas de la reciente encuesta que hemos realizado a profesionales de la seguridad de las aplicaciones: más de la mitad de las organizaciones emplea scripts de terceros predefinidos en las aplicaciones web. Cuando se utiliza código de terceros, debe prestarse especial atención a la seguridad, sobre todo cuando el código se envía a un navegador directamente desde la plataforma de origen, como GitHub. Si el código se ha manipulado, un ataque a la cadena de suministro de software, como Magecart, podría estar a la vuelta de la esquina. Las organizaciones deben llevar cuidado con este enfoque del desarrollo de aplicaciones.

Aproximadamente, ¿qué porcentaje del total de aplicaciones de su organización emplean scripts de terceros?

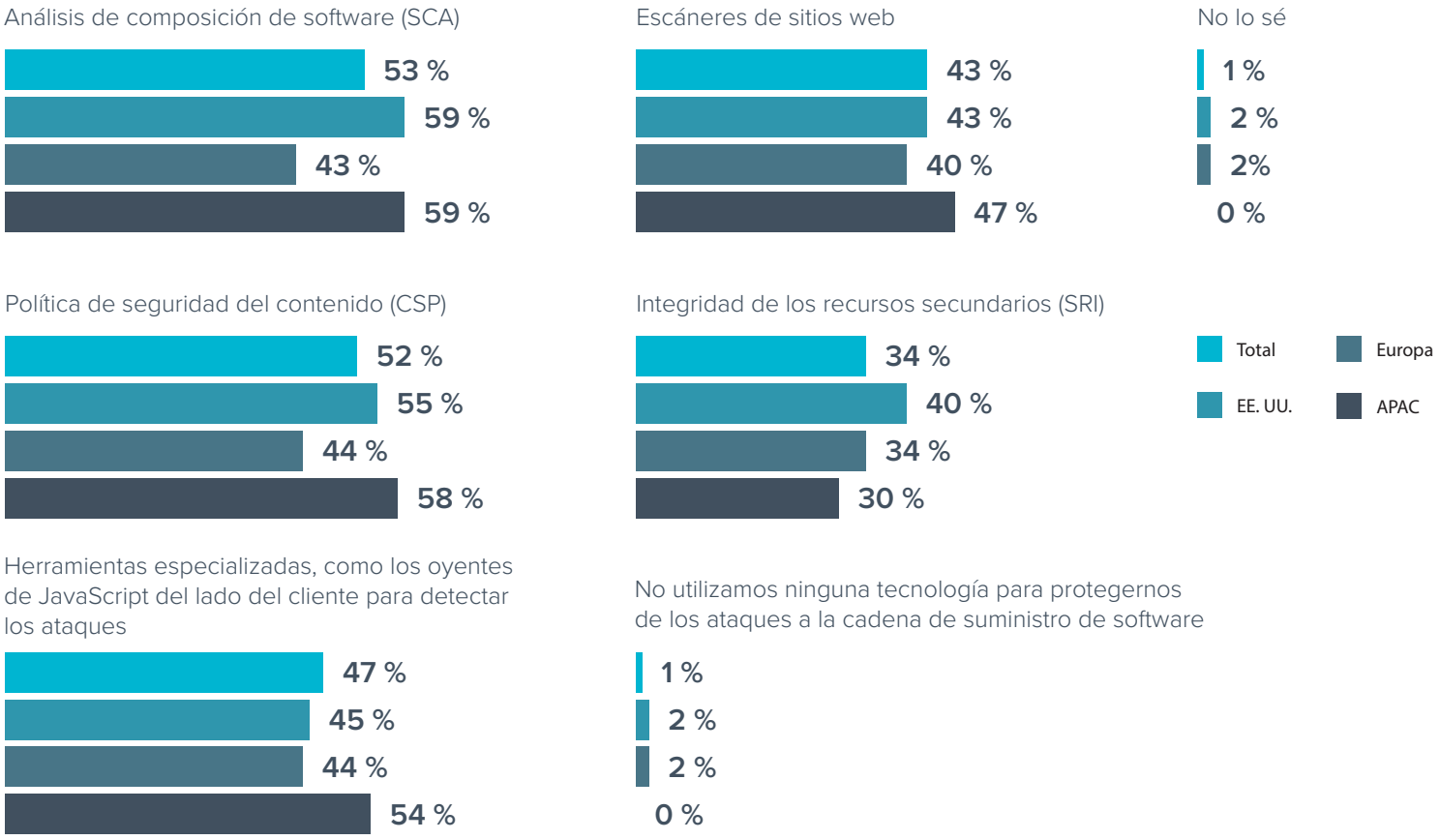
(n=750)



Existen medidas de protección relativamente estándares para mitigar los ataques a la cadena de suministro. Los encuestados de APAC son quienes más utilizan herramientas especializadas, como los oyentes de JavaScript del lado del cliente, para identificar este tipo de ataques. Con los oyentes, hay más probabilidades de detectar a los atacantes más avanzados que con los escáneres de sitios web. Estos son la cuarta tecnología más popular de esta lista, aunque se falsifican fácilmente, como demuestra el skimmer Baka descubierto por Visa. Por otro lado, la integridad de los recursos secundarios (SRI) es difícil de configurar y mantener, lo que podría explicar su baja popularidad.

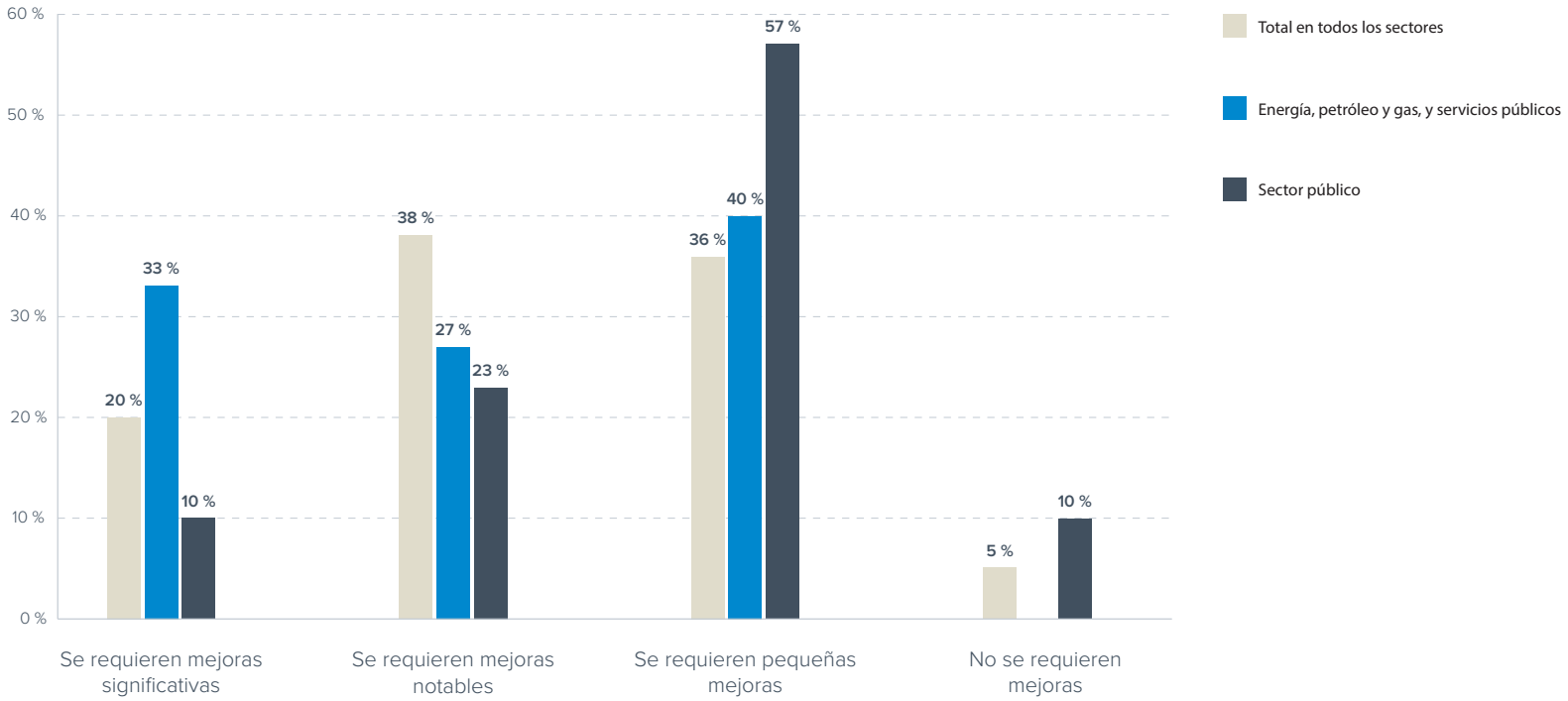
¿Qué tecnología emplea su organización para protegerse de los ataques a la cadena de suministro de software?

(n=750)



¿Qué nivel de mejora cree que debe alcanzarse en su organización en lo que respecta a la defensa frente a ataques a la cadena de suministro de software?

(n=728)



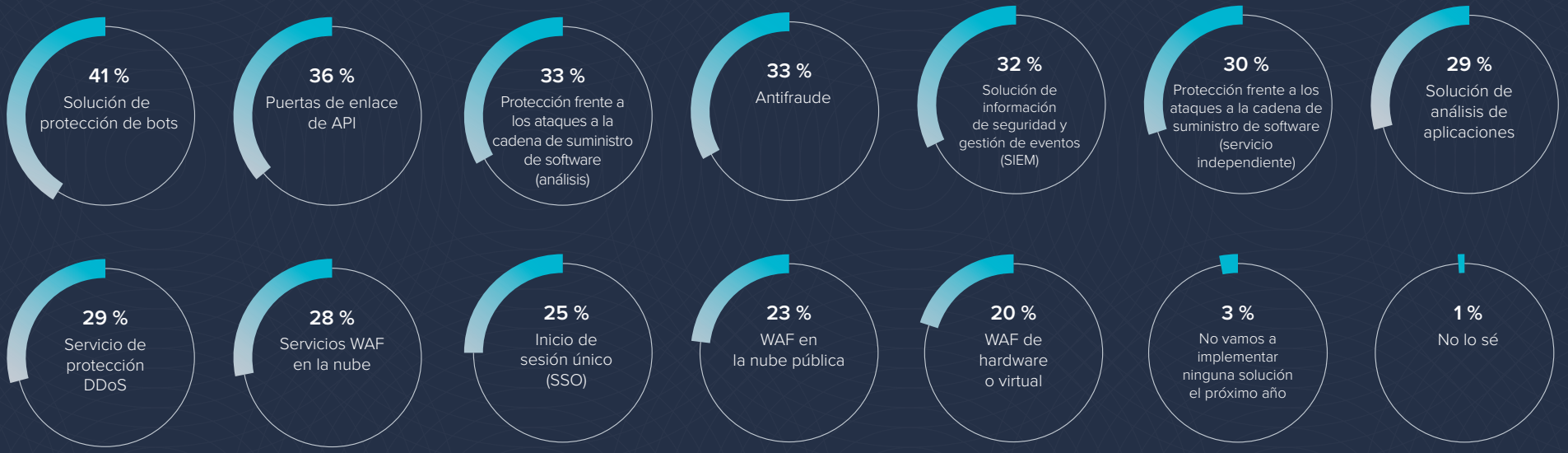
La mayoría de las organizaciones se encuentra dividida en lo relativo a las mejoras que precisan sus cadenas de suministro de sitios web. Los encuestados que trabajan en el sector público fueron los más propensos a afirmar que su protección requiere pequeñas mejoras o que no necesita ninguna mejora. Tan solo el sector de la energía, el petróleo, el gas y los servicios públicos indicó que se precisan mejoras significativas. Esto es más bien un reflejo de la corta vida de este vector de ataque, lo cual hace que su impacto no se entienda completamente. A medida que vayan saliendo a la luz más ataques de este tipo, el vector de ataque ganará más protagonismo.

Conclusión: preparación de cara al nuevo abecé de la seguridad de las aplicaciones

En la actualidad, las organizaciones están sufriendo más violaciones a través de sus aplicaciones web y API que nunca antes. A medida que proliferan las nuevas tecnologías, los atacantes buscan incansablemente formas de eludir sus medidas de seguridad y vulnerarlas. Las API, los ataques de bots y los ataques del lado del cliente son las últimas formas en las que están trabajando para vulnerar las aplicaciones por mera diversión o para obtener determinado beneficio.

¿Cuál de las siguientes soluciones implementará su organización en el próximo año?

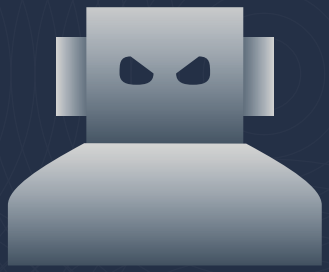
(n=750)



Barracuda

Según nuestra investigación, las organizaciones parecen estar entendiendo esto, ya que muchas tienen planeado implementar nuevas soluciones el próximo año, como la protección contra bots (41 %), la puerta de enlace de API (36 %) y la protección de la cadena de suministro de software (análisis) (33 %).

Es buena señal que las organizaciones se interesen en buscar soluciones para reforzar la seguridad de las aplicaciones, aunque a más soluciones, mayor complejidad presentará esta seguridad. La solución de seguridad de aplicaciones más eficaz es la que consiste en una plataforma capaz de proteger a los clientes contra todos estos vectores de ataque, de proporcionar gran protección contra las amenazas tradicionales y emergentes, y de ser fácil de usar y gestionar.



Sobre Barracuda

En Barracuda luchamos por hacer del mundo un lugar más seguro. Estamos convencidos de que toda empresa merece disfrutar de soluciones de seguridad cloud-first específicas para su labor que sean fáciles de adquirir, instalar y utilizar. Protegemos los correos electrónicos, las redes, los datos y las aplicaciones con soluciones innovadoras capaces de crecer y adaptarse a la experiencia de nuestros clientes. Más de 200 000 organizaciones en todo el mundo confían en Barracuda para su protección, a unos niveles a los que puede que ni ellas sepan que están en riesgo, de modo que puedan centrarse en llevar su negocio siempre un paso más allá. Para obtener más información, visite barracuda.com.

Barracuda