Akamai

Estado de Internet

Volumen 9 | Número 6

Resumen del año:

Una mirada a las cibertendencias de 2023 y lo que está por venir

Tabla de contenido

02 Historias sobre el terreno

03 El talón de Aquiles del sector sanitario: los peligros cibernéticos del Internet de las cosas médicas

05 Descubrimiento de las grandes amenazas de la identificación de API con JSON Web Tokens

07 Vulnerabilidad de omisión de Outlook

09 Nuevos datos y amenazas emergentes: damos la voz de alarma sobre los ataques de Magecart

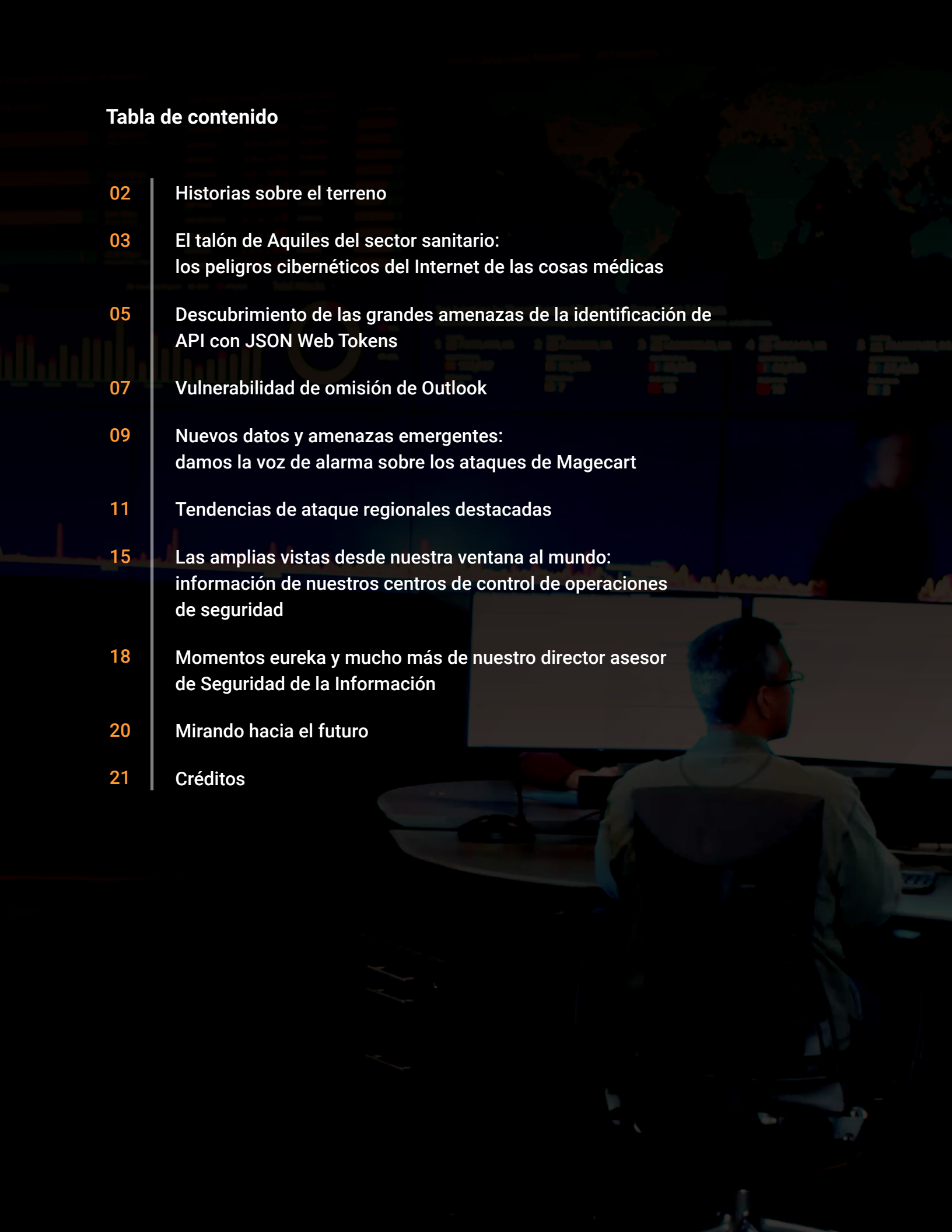
11 Tendencias de ataque regionales destacadas

15 Las amplias vistas desde nuestra ventana al mundo: información de nuestros centros de control de operaciones de seguridad

18 Momentos eureka y mucho más de nuestro director asesor de Seguridad de la Información

20 Mirando hacia el futuro

21 Créditos



Historias sobre el terreno

En este informe sobre el estado de Internet (SOTI), nos alejamos del típico resumen de final de año en el que hablamos de cada uno de los informes anteriores publicados ese año y, en su lugar, nos centramos en este tema principal: ¿Cuál es su historia favorita del año en cuanto a la seguridad se refiere? Pedimos a los redactores y a una especialista en datos del grupo de inteligencia sobre seguridad (SIG) de Akamai que hicieran una evaluación de fin de año de las historias que contamos a lo largo de los últimos 10 meses. Seguro que les ha resultado difícil elegir solo uno de los numerosos descubrimientos e historias de gran interés que publicamos en nuestro blog de investigación sobre seguridad y en los SOTI de 2023. También hemos pedido a nuestro director asesor de Seguridad de la Información y a un vicepresidente de nuestros centros de control de operaciones de seguridad (SOCC) que nos den su opinión sobre las tendencias de ataque de este año y las lecciones que podemos sacar de cara a 2024.

Este año han pasado muchas cosas en el mundo de la seguridad y en el contexto de la investigación en materia de seguridad de Akamai. Sin duda, las aportaciones de nuestros expertos en seguridad tienen un valor incalculable para la comunidad. A través de nuestro centro específico, los profesionales de la seguridad pueden acceder fácilmente a recursos de confianza que contienen información, estrategias de mitigación y tendencias de ataque que pueden ayudarles a defender a sus organizaciones. También pueden acceder a herramientas gratuitas, como nuestro kit de herramientas de RPC, así como a nuestra plataforma de emulación de adversarios gratuita y de código abierto, Infection Monkey. Infection Monkey actúa como si fuera malware, es decir, propaga y "cifra" los archivos a los que puede acceder cambiando los bits, lo que proporciona a los profesionales una panorámica realista de cómo un atacante podría (o no podría) moverse por ese entorno. Debido a la velocidad a la que evolucionan las amenazas, es imprescindible hacer pruebas continuamente. Los profesionales necesitan saber en qué estado se encuentra su red en la actualidad, no solo el que tenía durante la última prueba de penetración.

Si hay una palabra que pueda definir el panorama en 2023, sería *adaptación*. Los atacantes han cambiado sus tácticas para eludir las medidas de seguridad, en busca de nuevas superficies de ataque y objetivos sin explotar para causar estragos en organizaciones de todos los tamaños y sectores. Lo mismo podría decirse de los equipos de seguridad, que siguen recalibrando y aprendiendo nuevas formas de mitigar los ataques y proteger mejor a las organizaciones. Adaptamos las soluciones, la investigación y las herramientas con el siguiente objetivo: proporcionar información útil y estrategias de mitigación a los profesionales de la seguridad que luchan contra las mismas amenazas de seguridad que nosotros.

¡Feliz lectura!

Historias de seguridad favoritas

Tendencias de ataque de 2023

2024: Mirando hacia el futuro

El talón de Aquiles del sector sanitario: los peligros cibernéticos del Internet de las cosas médicas

Soy Badette Tribbey, una de las autoras de los informes SOTI, y colaboro con expertos en seguridad y especialistas en datos para transformar los hallazgos técnicos y los datos en información útil. No me gustan nada las matemáticas, pero me encanta constatar que los números pueden revelar tendencias de ataque convincentes.

Uno de los temas más destacados que hemos tratado este año nos toca de cerca: el incremento de los riesgos del Internet de las cosas médicas (IoMT). En Atravesando las brechas de seguridad y El ransomware en movimiento, examinamos el panorama de riesgos del sector sanitario y de las ciencias de la vida y por qué ese sector es susceptible a los ataques. Una de las cosas que más me llamó la atención es cómo los activos de IoMT, como máquinas de IRM, bombas de insulina y dispositivos portátiles, aunque son muy beneficiosos para los pacientes, han elevado de forma significativa los riesgos de los proveedores de atención sanitaria. Estas organizaciones ya se enfrentaban a desafíos para proteger su perímetro debido a la complejidad del ecosistema sanitario, la vulnerabilidad de la tecnología heredada y los problemas de dotación de personal de TI y ciberseguridad. Además, la aplicación oportuna de parches en este entorno puede ser una tarea hercúlea, con actualizaciones procedentes de distintos proveedores para diferentes sistemas o aplicaciones, lo que dificulta su seguimiento.

Los dispositivos IoMT sin parches aplicados son algunos de los activos más vulnerables en todos los sectores y pueden introducir amenazas más nefastas, como el ransomware. Con el crecimiento exponencial del IoMT y, con ello, el uso de API, sus vulnerabilidades también crecen y pueden convertirse en vías para que los atacantes se infiltren en sus objetivos o los vulneren, lo que puede provocar filtraciones de datos (figura 1). Un informe conjunto de Cynerio y Ponemon Institute sobre un estudio realizado en varios hospitales y sistemas sanitarios de Estados Unidos indicó que más de la mitad sufrió ciberataques como resultado de brechas de seguridad en los dispositivos IoMT.

> “La aplicación oportuna de parches en el entorno [sanitario] puede ser una tarea hercúlea, con actualizaciones procedentes de distintos proveedores para diferentes sistemas o aplicaciones, lo que dificulta su seguimiento.
>
> **– Badette Tribbey, Redactora técnica sénior, Akamai**

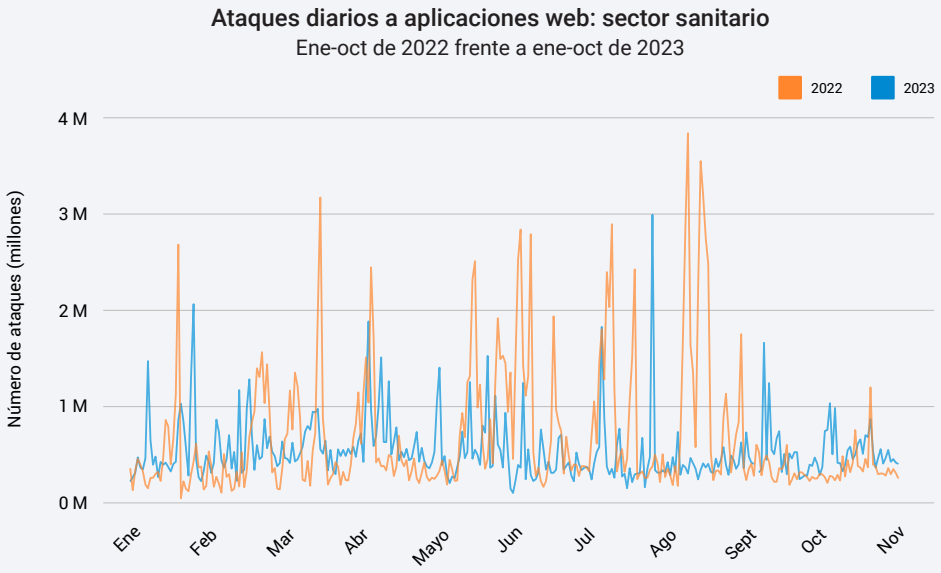


Fig. 1: Los ataques a las API y aplicaciones web en el sector sanitario y farmacéutico muestran una actividad constante con picos esporádicos entre 2022 y 2023. Aunque los ataques han ido disminuyendo un 21 % de año en año, el promedio de ataques diarios en 2023 es superior al de 2022.

Qué podemos esperar en el sector sanitario

A medida que el sector sanitario amplía su IoMT, las API seguirán desempeñando un papel esencial en la accesibilidad de los servicios médicos (por ejemplo, la telesalud y la monitorización remota de pacientes), lo que se traducirá en mejores resultados clínicos y financieros. Asimismo, es probable que los ataques contra el sector sanitario no se ralenticen, debido al gran valor que tienen los historiales médicos y los datos de pacientes en la Dark Web.

Más allá de lo que ha estado pasando, si nos fijamos en lo que podemos esperar, es evidente que los atacantes seguirán innovando y aumentando el alcance y la complejidad de sus ataques. Es probable que constatemos una tendencia continuada hacia ataques más técnicos que aprovechen las vulnerabilidades de día cero. Además, el panorama normativo (incluida, entre otras, la ley estadounidense sobre protección y transformación de la atención sanitaria cibernética [PATCH] de 2022) está cambiando, por lo que debemos asegurarnos de que nuestras soluciones puedan ayudar a cumplir un gran volumen de leyes de próxima aprobación sobre privacidad, informes, pagos, soberanía de datos y resiliencia. Por último, esperamos que haya más interrupciones en los ataques para los directores de seguridad de la información (CISO) que cambien los presupuestos para consolidarse en menos proveedores y utilizar soluciones que minimicen el tiempo de permanencia de los hackers que se han infiltrado.

Descubrimiento de las grandes amenazas de la identificación de API con JSON Web Tokens

Soy Lance Rhodes y tengo el placer de formar parte del equipo de SIG de Akamai como redactor en materia de ciberseguridad desde marzo de 2023. Gran parte de mi trabajo sirve de "tejido conectivo" entre nuestros informes y blogs, ya que trabajo tanto en los aspectos de publicación como de redacción de las entradas de blog y los apartados de investigación, además de en la redacción de contenido y materiales de marketing para los informes SOTI. Y todo esto se une en mi colaboración con el equipo en nuestros boletines internos y externos mensuales y en las propuestas presentadas en conferencias sobre seguridad.

Diría que una de las entradas del blog más interesantes en las que he trabajado este año fue la que trataba sobre JSON Web Token (JWT). Esta entrada tenía una conexión directa con el informe SOTI sobre aplicaciones y API (Atravesando las brechas de seguridad), en el sentido de que ampliaba la información sobre la autenticación comprometida en los JWT, uno de los métodos de identificación estándar de las API. Por lo tanto, fue muy interesante poder conocer más a fondo los JWT.

Después de trabajar en el informe SOTI sobre aplicaciones y API a principios de año, empecé a colaborar con Nitzan Namer en la entrada sobre JWT, que se centró en JWT como vector de ataque para la autenticación de usuarios comprometida, una de las 10 principales vulnerabilidades de seguridad de API según el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP). El informe SOTI tenía una sección específica dedicada a esto, pero la entrada del blog profundizaba en la estructura de JWT y las prácticas recomendadas para protegerse contra las amenazas de mayor envergadura, incluidas la escalada de privilegios, la filtración de datos y el robo de cuentas.

Recuerdo que comenté con Nitzan que teníamos la esperanza que la entrada se utilizara como recurso de consulta continua para investigadores de seguridad, profesionales técnicos, y usuarios y administradores de JWT. La entrada ha satisfecho nuestras expectativas gracias a su estilo estructural: los aspectos básicos de JWT se enumeran en primer lugar, seguidos de seis escenarios posibles, que incluyen ilustraciones que ejemplifican algunas amenazas habituales y señalan las prácticas recomendadas para cada una. Los aspectos básicos incluyen información sobre cómo los JWT protegen las API mediante la emisión de tokens que contienen información para compartirse como objetos JSON. Cada token está codificado, aunque no cifrado, y consta de un encabezado, carga y firma de verificación (certifica que los datos no se han alterado desde que el servidor falsificó el token).

> “La entrada del blog profundizaba en la estructura de JWT y las prácticas recomendadas para protegerse contra las amenazas de mayor envergadura, incluidas la escalada de privilegios, la filtración de datos y el robo de cuentas.
>
> **– Lance Rhodes, Redactor en materia de ciberseguridad, Akamai**

Los seis escenarios son:

1. Permitir que el servidor utilice un token sin validación
2. Utilizar la misma clave privada para diferentes aplicaciones
3. Utilizar un algoritmo de firma débil
4. Elegir una clave privada de entropía corta o baja
5. Mantener datos confidenciales en la carga de un JWT
6. Confundir las claves

Los JWT son uno de los formatos de verificación más habituales y las medidas de seguridad adecuadas son cruciales, ya que el formato proporciona una gran superficie de ataque con mucho margen para errores. Aunque estos escenarios muestran algunas de las amenazas más habituales a las que se enfrentan los JWT, hay muchas más y las técnicas de ataque están en constante evolución.

Los JWT no se cifran ni se implementan pensando en la seguridad

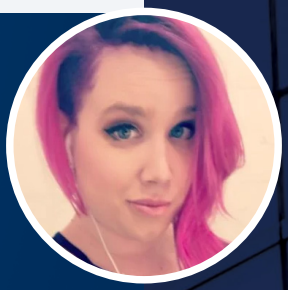
Una de las principales conclusiones que saqué de la entrada del blog es que los JWT no se cifran ni se implementan pensando en la seguridad. Cuesta creer que un token de autenticación tan popular pueda ser tan vulnerable. Parte del atractivo de los JWT es que permiten el uso de muchas aplicaciones web y API sin tener que iniciar sesión con frecuencia. Tanto el informe SOTI como la entrada del blog sobre JWT analizaron los algoritmos JWT en el tráfico de Akamai y determinaron que los algoritmos simétricos son los más habituales, aunque en teoría son menos seguros y no protegen tanto como los algoritmos asimétricos. Por ejemplo, en ambas publicaciones se constata que el 54,8 % de los clientes de Akamai utiliza el algoritmo HS256, que es simétrico.

Es probable que los algoritmos simétricos se elijan más a menudo porque el usuario solo necesita una clave y los algoritmos asimétricos requieren una mayor cantidad de recursos informáticos. El uso de JSON Web Encryption (JWE), que es la versión cifrada de JWT, tampoco está generalizado. La mayoría de las empresas se decantan por JWT y deciden ahorrar en capacidad informática.

Conclusión: la simplicidad, el coste y la velocidad suelen priorizarse por encima de la seguridad. Este es un valioso recordatorio de la importancia de nuestro trabajo como investigadores y redactores en materia de seguridad. Se necesitan buenas investigaciones y prácticas de seguridad para lograr un equilibrio satisfactorio entre la eficiencia y la seguridad.

> Cuesta creer que un token de autenticación tan popular pueda ser tan vulnerable.
>
> – Lance Rhodes, Redactor en materia de ciberseguridad, Akamai

Vulnerabilidad de omisión de Outlook



¡Hola! Espero que el día le haya sonreído. Me llamo Tricia Howard y trabajo en el blog del SIG. Vivo en el meollo de los informes técnicos y colaboro con nuestros investigadores, nuestro equipo de comunicaciones corporativas y nuestro departamento jurídico (entre otros) para que los textos se publiquen de forma oportuna y eficaz. Lo mejor de mi trabajo es que tengo la oportunidad de presumir en nombre de nuestros investigadores, porque lo que hacen es estupendo.

De todo sobre lo que me han pedido que escriba este año, puede que esto sea lo más difícil. De entre todas las cosas increíbles que nuestro equipo ha hecho en los últimos 12 meses, me resulta complicadísimo elegir mi favorita. Pero como tengo que elegir solo una, me decanto por el trabajo de Ben Barnea sobre la famosa (o, mejor dicho, infame) vulnerabilidad de omisión de Outlook. Ben es uno de los investigadores más brillantes que conozco y logró encontrar una manera de comprometer un parche entero… con una simple barra. Sé que parece absurdo, incluso imposible, pero era posible y lo hizo.

La vulnerabilidad original permitía a un atacante no autorizado enviar una invitación de Outlook con un sonido de notificación personalizado. Este sonido también servía de ruta de ataque que permitía establecer una conexión al servidor del atacante, proporcionando credenciales NTLM. Esto es terrible: a partir de ahí, el atacante puede usar un ataque de fuerza bruta para obtener las credenciales o ejecutar un ataque de retransmisión. Por supuesto, todo esto puede llevar a la derivación de privilegios, y todos sabemos lo que puede pasar cuando sucede esto. Lo peor de todo es que esta vulnerabilidad era sin clics, lo que significa que el usuario no tenía que hacer nada para ejecutar el ataque. Así, algo que ya es potente de por sí se convierte en algo sumamente peligroso, sobre todo cuando se descubre que se originó en Rusia y que se utilizó a gran escala, infiltrándose en varios organismos gubernamentales europeos.

El parche se publicó en marzo y eliminaba la posibilidad de utilizar *PidLidReminderFileParameter*, que es lo que permitía al atacante especificar la ruta personalizada (es decir, conectarse al servidor de la persona con malas intenciones). En su lugar, el parche utilizaba la función *MapURLtoZone*, que comprobaba si la ruta intentaba conectarse a Internet. Si se intentaba establecer una conexión, se reproducía el sonido de notificación tradicional, lo que eliminaba la opción de especificar una ruta de archivo para la notificación personalizada. En teoría, esto eliminaría la opción de que un atacante remoto aprovechara esta vulnerabilidad: tendría que acabar haciendo una llamada a Internet para establecer una conexión entre el atacante y la víctima.

> Los equipos de seguridad ya tienen suficiente trabajo cada día sin nuevas vulnerabilidades de escalada de privilegios sin clics por las que preocuparse.
>
> **– Tricia Howard, Redactora técnica sénior, Akamai**

Neutralizar el parche

Aquí es donde el asunto se pone interesante y, si se me permite decirlo, bastante gracioso. Como cualquier excelente investigador, Ben quería verificar que, en efecto, la vulnerabilidad ya no podía explotarse. Aunque es simplificarlo muchísimo, *MapURLtoZone* tiene dos opciones, básicamente: permitir o denegar. ¿Llama a Internet o no? En general, el parche funcionaba como estaba previsto. Incluso cuando la ruta parecía ser local, *MapURLtoZone* reconocía que tenía la intención de conectarse a Internet y le impedía hacerlo.

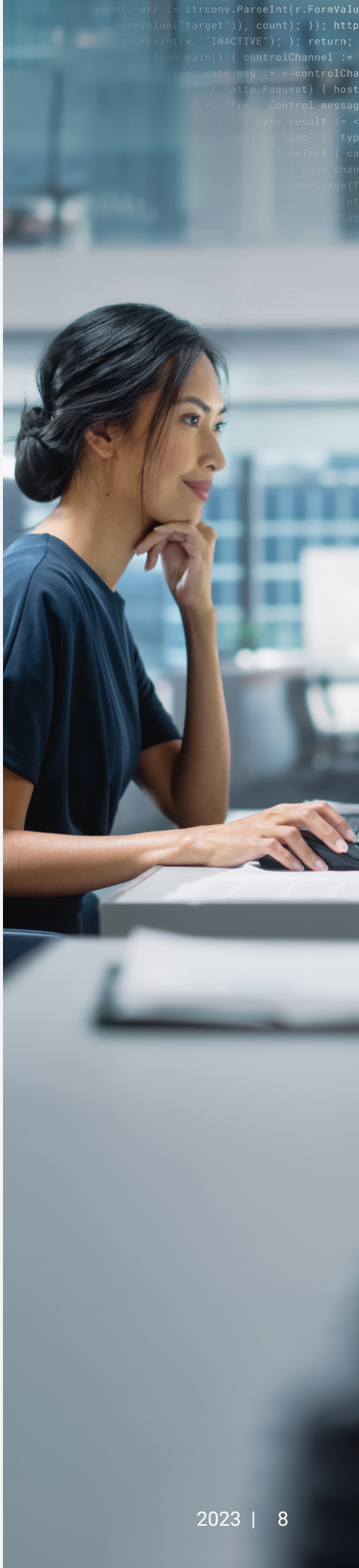
Ben decidió experimentar con el nombre de la ruta añadiéndole "/" al final. Aunque se proporcione algo que *MapURLtoZone* no espera, la función tiene que decidir si lo permite o lo deniega. La barra adicional no se reconoció, lo que a su vez devolvió un 0, que la función leyó como local y de confianza. Después de eso, el resto de la vulnerabilidad pudo ejecutarse exactamente de la forma en que estaba prevista, utilizando *CreateFile* para la ruta personalizada.

¡No hizo falta más! Se añadió una simple barra y todo un parche para una vulnerabilidad **crítica** dejó de ser una solución eficaz. Es probable que el parche se creara tras días, posiblemente semanas o meses, de tiempo y energía de profesionales de la ciberseguridad para eliminar esta amenaza… para acabar siendo frustrado por una sola barrita.

Cuando analizas el ataque original, su extrema sofisticación resulta impresionante. El atacante está jugando una partida larga del nivel de Magnus Carlsen. Teniendo en cuenta que solo se necesitó una barra para que el parche resultara inútil, es lógico pensar que los atacantes hubieran acabado descubriendo cómo omitirlo por sí solos. Es estupendo que fuera Ben quien lo descubrió yendo más allá de lo convencional.

Por eso, los investigadores que descubren estos errores son el alma de la comunidad de seguridad. Los equipos de seguridad ya tienen suficiente trabajo cada día sin nuevas vulnerabilidades de escalada de privilegios sin clics por las que preocuparse. Los investigadores de seguridad están marcando una diferencia real en el mundo, especialmente a medida que dependemos cada vez más de la tecnología y de Internet en nuestra vida diaria.

Me enorgullece mucho formar parte de este increíble equipo y trabajar con algunas de las mentes más privilegiadas del mundo. A las personas que han leído nuestros blogs, publicaciones en X (anteriormente, Twitter) y SOTI: gracias. Y a los investigadores, tanto dentro como fuera del SIG de Akamai: gracias por todo lo que hacen, problematizan y descubren. Ya veremos qué nos deparará el próximo año.



Nuevos datos y amenazas emergentes: damos la voz de alarma sobre los ataques de Magecart

Soy Chelsea Tuttle y llevo trabajando en Akamai casi ocho años. Como especialista en datos responsable de los datos representados en el SOTI durante los últimos cuatro años, paso la mayoría del tiempo limpiando, explorando, analizando y visualizando nuestros datos. Cuando no estoy observando datos, colaboro estrechamente con los redactores del SOTI para ayudarles a comunicar las historias que nos cuentan nuestros datos. Debido a la complejidad del big data y a las ventajas de informar sobre datos históricos, no solemos añadir un nuevo conjunto de datos, pero este año lo hemos hecho. Cuando rememoro lo que ha pasado en 2023, pienso en los artículos que hemos publicado en torno a este nuevo conjunto de datos. Se encuentran entre mis historias favoritas porque me han encantado las oportunidades de aprendizaje que han acompañado a este empeño.

Con demasiada frecuencia, en nuestro mundo nos centramos en informar sobre el número de intentos de ataque que observamos en nuestra red y nos perdemos oportunidades importantes para informar de datos relevantes para protegernos frente a las posibles vulnerabilidades e impedir ataques. Un conjunto de datos que hemos añadido a nuestros informes SOTI de este año destaca porque es el único que resalta una posible área de vulnerabilidad en lugar de centrarse en el volumen de ataques. Este conjunto de datos se deriva de las observaciones proporcionadas por Client-Side Protection & Compliance de Akamai a partir de su visión avispada de miles de millones de scripts de páginas web a diario. Una de las áreas de posible vulnerabilidad que vigilamos es el número de scripts propios y de terceros utilizados en los sitios web. Aunque el uso de un script propio no garantiza la seguridad y el uso de un script de terceros no garantiza una vulnerabilidad, cuanta más confianza se deposite en otra persona, como confiar en un tercero para alojar un script de página web, más riesgo se añade a un perfil de seguridad. Akamai se esfuerza por salvar la brecha entre practicidad y seguridad que se ha creado debido al creciente uso de scripts de terceros en todos los sectores.

> “Akamai se esfuerza por salvar la brecha entre practicidad y seguridad que se ha creado debido al creciente uso de scripts de terceros en todos los sectores.
>
> **– Chelsea Tuttle, Especialista sénior en datos, Akamai**

Como se ve en nuestro informe SOTI Análisis de las tendencias de las amenazas en el sector del comercio de junio de 2023, una de las áreas de interés de la investigación de Akamai de este año han sido los recientes ataques de robo de información web de tipo Magecart; en concreto, hemos observado cómo los ataques de Magecart siguen invadiendo el sector del comercio digital. Este tipo de ataque intenta robar credenciales de usuario confidenciales, como la información de la tarjeta de crédito, del carrito de compra de un sitio web de comercio digital mediante la inyección de código JavaScript malicioso. Este tipo de ataque tiende a ser fácil para los adversarios, pero presenta enormes riesgos para los consumidores y cada vez es más difícil de detectar. Estos ataques de Magecart, o de robo de información

web, se producen a menudo sin que el usuario o el propietario del sitio web se den cuenta siquiera y los atacantes suelen elegir sitios web de comercio digital que utilizan software vulnerable u obsoleto.

Variantes recientes de Magecart

En las campañas más recientes de Magecart analizadas por los investigadores de Akamai, se observan unas cuantas variantes de Magecart. Nuestro informe SOTI de junio de 2023 se centró en los ataques de Magecart del lado del cliente y señaló las vulnerabilidades explotadas encontradas en scripts de terceros de bibliotecas de código abierto que podrían conducir a ataques a la cadena de suministro. Poco después de redactar ese informe SOTI, publicamos una entrada del blog sobre cómo los investigadores de Akamai descubrieron una nueva campaña de tipo Magecart que se valía de sitios web legítimos para atacar a otros. Esa campaña tenía básicamente dos conjuntos de sitios web como víctimas: los sitios legítimos secuestrados para el alojamiento, que actúan como servidores controlados por el atacante, y los sitios de comercio vulnerables atacados, con robo de información web del lado del cliente. En agosto se publicó una segunda entrada del blog en la que se describía cómo los investigadores de Akamai descubrieron otra nueva campaña contra Magento con inyección de plantillas ocultas en el lado del servidor que explotaba los sitios de comercio digital para obtener estadísticas de pago de las víctimas.

Los investigadores de Akamai han descubierto una nueva campaña de tipo Magecart que se valía de sitios web legítimos para atacar a otros

La entrada del blog más reciente sobre Magecart del SIG de Akamai revela una nueva técnica de ofuscación en la que los atacantes manipulan la página de error 404 predeterminada del sitio web para ocultar código malicioso. Los investigadores de Akamai descubrieron que esta nueva campaña consiste en dos técnicas avanzadas de ocultación adicionales y presentaron las tácticas en desarrollo que los atacantes utilizan para alargar la cadena de ataque y evitar la detección.

Ahora que nos acercamos al final de 2023 y rememoro todas las oportunidades de investigación y generación de informes que hemos tenido gracias a los nuevos datos y las amenazas emergentes, no puedo evitar sino estar deseando ver los nuevos datos y las oportunidades de aprendizaje que nos deparará 2024.

Tendencias de ataque regionales destacadas

Soy Charlotte Pelliccia y me incorporé al equipo de SOTI en 2023 para sacar a la luz las historias de las regiones de Asia-Pacífico y Japón (APJ) y Europa, Oriente Medio y África (EMEA). Nuestras instantáneas de APJ y EMEA son documentos complementarios a nuestros informes SOTI de ámbito mundial. Aquí, repasaré algunas de las tendencias de ataque más importantes que hemos tratado en 2023 y actualizaré los datos de las instantáneas publicadas a principios de año.

Ataques a aplicaciones web y API: una historia de dos sectores

En consonancia con nuestros informes SOTI sobre servicios financieros y comercio más recientes, los servicios financieros han seguido siendo el principal sector objeto de los ataques a aplicaciones web y API en APJ, seguido del comercio. Desde nuestro informe de junio de 2023, los ataques a los servicios financieros han superado los 4500 millones (respecto a 3700 millones, lo que supone un aumento del 22 %). Y desde nuestro informe de marzo de 2023, los ataques al comercio han aumentado de 1200 millones a 1900 millones, lo que supone un incremento del 58 %. El reparto entre subsectores sigue siendo relativamente constante (figura 2).

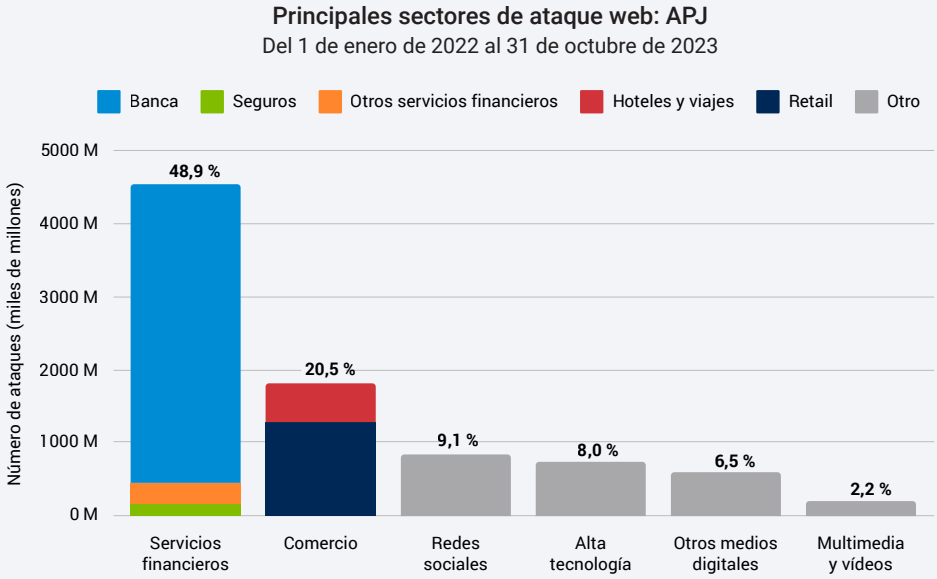


Fig. 2: Sectores objeto de ataques web en APJ hasta octubre de 2023

> La visibilidad de las tendencias de ataques regionales resulta fundamental para ayudar a las organizaciones a conocer mejor sus riesgos y a ajustar sus herramientas y prácticas recomendadas.
>
> **– Charlotte Pelliccia, Redactora en materia de ciberseguridad, Akamai**

Mientras tanto, en EMEA, el comercio sigue siendo el principal sector objeto de los ataques a aplicaciones web y API, cuya cifra ya supera los 6500 millones (respecto a 4600 millones, un aumento del 41 %) desde nuestro informe de marzo de 2023. Aunque el sector de la fabricación ha subido desde el cuarto puesto y ha sustituido a los servicios financieros en el tercer puesto, los ataques contra los servicios financieros han aumentado un 70 % desde el informe de junio de 2023 y ascienden a 1700 millones, respecto a los 1000 millones de aquel informe. También en este caso, el reparto entre subsectores se ha mantenido relativamente constante (figura 3).

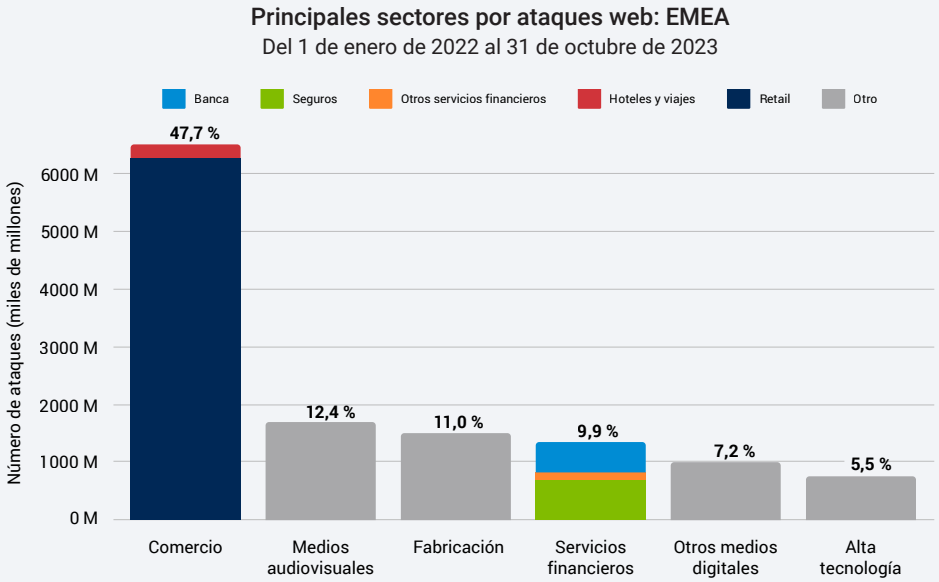
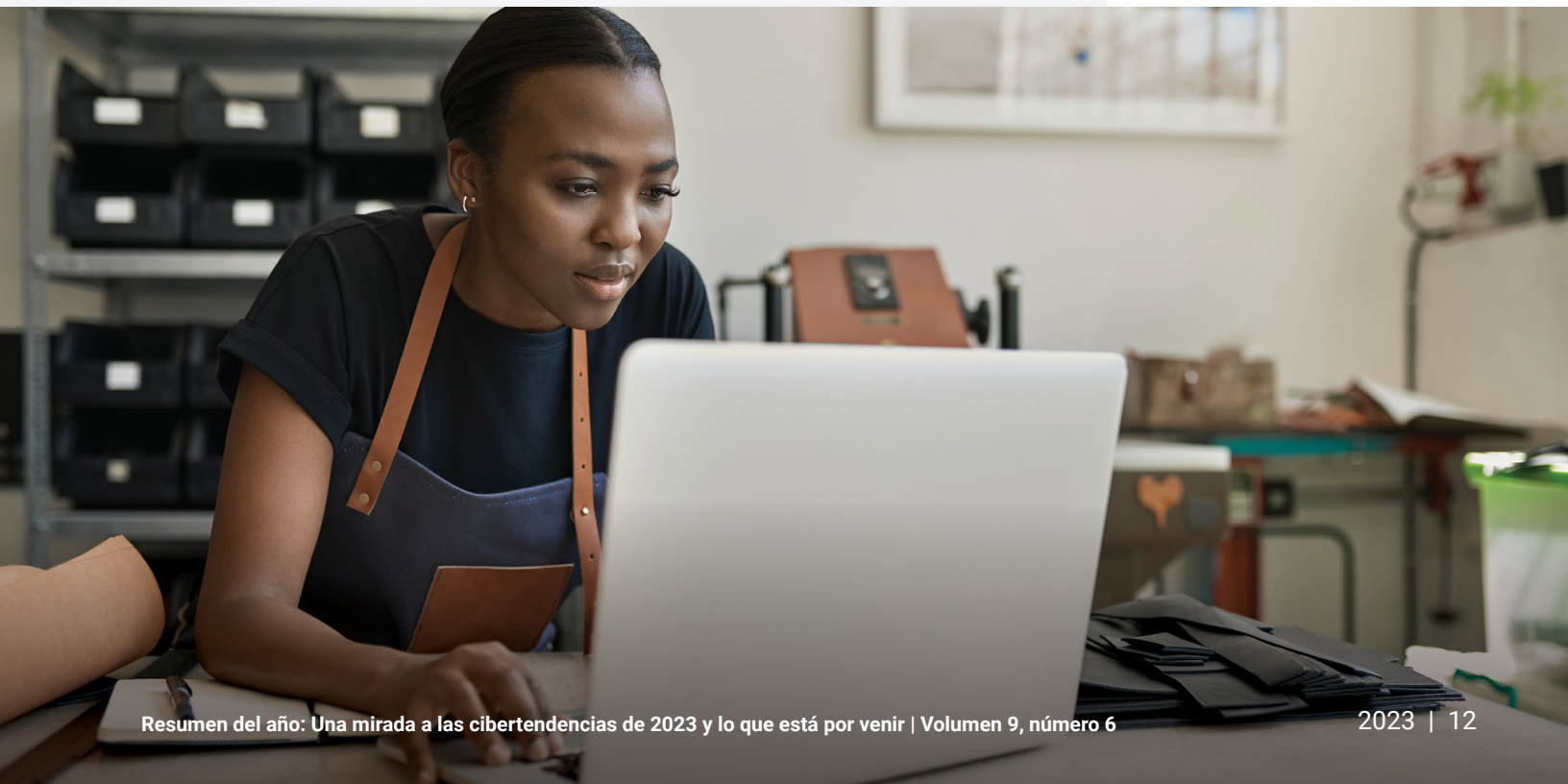


Fig. 3: Sectores objeto de ataques web en EMEA hasta octubre de 2023



Los bots maliciosos son una de las armas preferidas

Siguiendo con lo que vimos en informes anteriores, APJ es la segunda región, tras Norteamérica, en lo que a actividad de bots maliciosos se refiere. Entre enero de 2022 y octubre de 2023, los tres principales sectores objeto de ataques en APJ fueron el de comercio (27,4%), multimedia y vídeo (15,0%) y servicios financieros (14,3%). En EMEA, la mitad (50,1 %) de toda la actividad de bots maliciosos se dirigió al comercio, seguido de otros medios digitales, con un 15,3 %, y de multimedia y vídeo, con un 12,2 % (figura 4).

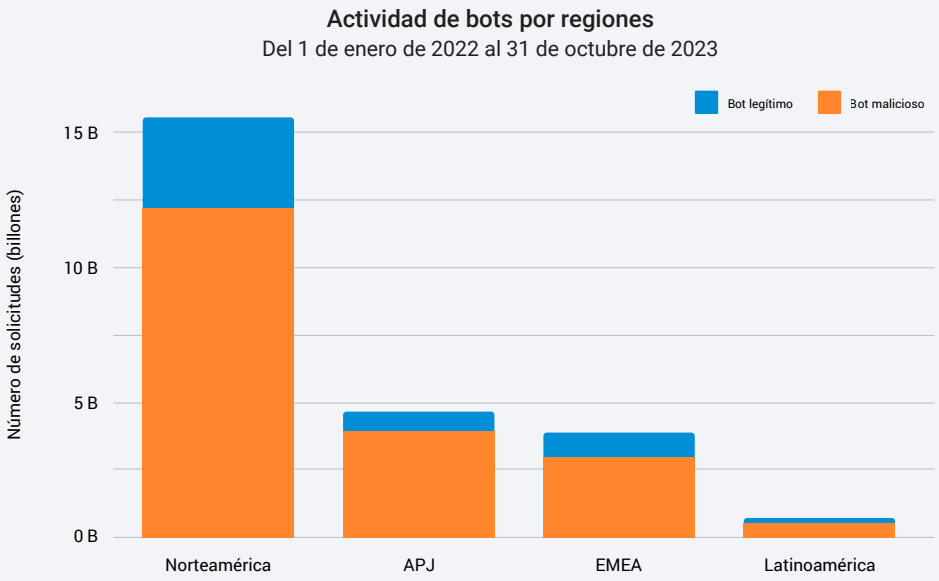


Fig. 4: El uso de bots maliciosos es prevalente en todas las regiones, superando con creces el uso de bots benignos.

> Lea el siguiente ensayo para obtener información de nuestro SOCC sobre cómo están cambiando los ataques de bots y DDoS.

EMEA en el punto de mira del cambio regional en los ataques DDoS

Nuestro informe de 2023 dejó muy claro que los atacantes han puesto en el punto de mira de lleno a EMEA, lo que puede atribuirse en parte a la situación geopolítica actual. Un ejemplo excelente: la cifra de ataques distribuidos de denegación de servicio (DDoS) contra los sectores de los servicios financieros, los juegos de apuestas y la fabricación en EMEA superó a la del resto de las regiones juntas (figura 5).

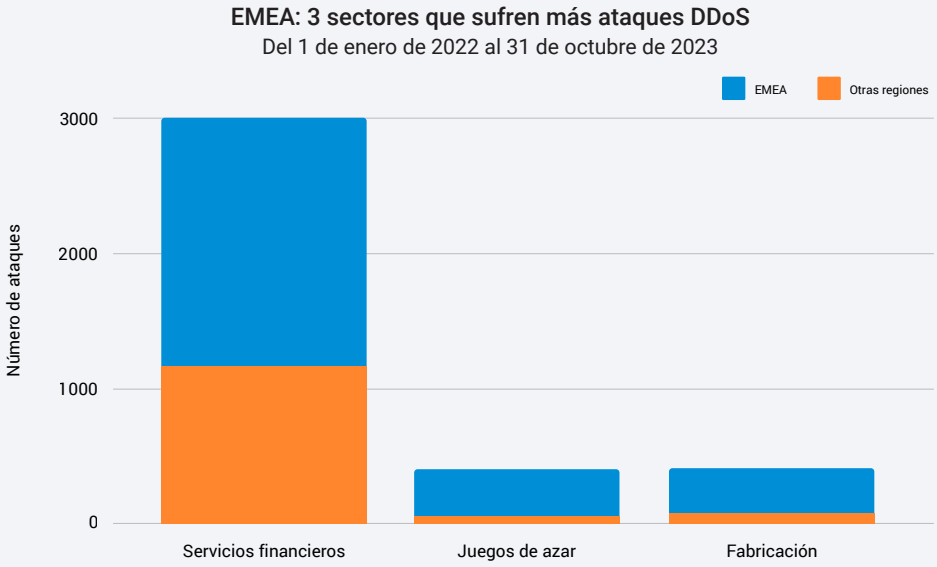


Fig. 5: EMEA experimentó más ataques DDoS en estos sectores que el resto de las regiones juntas.

Una mirada hacia el futuro

Siempre que los atacantes se salgan con la suya con los ataques web, de bots y DDoS, es razonable esperar que estas sigan siendo sus armas preferidas. De hecho, estos tres vectores ya están evolucionando para mantenerse o cobrar fuerza. Las vulnerabilidades de día cero de las aplicaciones web se están entrelazando con las técnicas de ransomware (por parte de grupos de ransomware como CL0P) e incluyen ataques DDoS para crear una táctica de triple extorsión. La reventa web a través de bots afecta de forma cotidiana a casi todos los eventos importantes de las aerolíneas o la venta de entradas. Y los ataques de API dirigidos a la lógica empresarial de las API son cada vez más frecuentes.

Como respuesta, las obligaciones normativas de supervisión y presentación de informes siguen aumentando en todo el mundo y en todos los sectores, ya que no hay ninguna región ni ningún sector a salvo de los ataques. El objetivo es mantener la legislación sobre ciberseguridad al día del cambiante panorama de amenazas. Las organizaciones deben estar atentas a la hora de cumplir los requisitos de presentación de informes y estar preparadas para mitigar el riesgo mediante una defensa multicapa.

Las amplias vistas desde nuestra ventana al mundo: información de nuestros centros de control de operaciones de seguridad

Soy Roger Barranco, vicepresidente de Operaciones Globales de Seguridad. Llevo trabajando en Akamai casi doce años y soy responsable de las operaciones de seguridad gestionadas de la empresa, las cuales atiende un equipo fantástico desde seis SOCC distribuidos por todo el mundo. Comencé mi trayectoria profesional en la ciberseguridad, un campo que me atrajo porque es un mercado interesante y en constante cambio. El año 2023 es un excelente ejemplo de ello.

El SOCC de Akamai nunca ha estado tan ocupado: a finales de 2023, habremos gestionado aproximadamente un 30 % más de tickets relacionados con la seguridad que el año pasado. Esta es la información clave que hemos obtenido al trabajar con nuestros clientes de servicios de seguridad gestionados y que las organizaciones deberían tener en cuenta de cara a 2024.

Los ataques DDoS están cambiando

Aunque la cifra de clientes que son objeto de ataques ha aumentado históricamente año tras año, el "cómo" es diferente en la actualidad. En primer lugar, el tipo y el volumen de las propiedades de clientes que son víctimas de ataques han cambiado. Por ejemplo, en lugar de 10 ataques contra los mismos terminales o similares, ahora vemos 100 ataques dirigidos a diferentes IP en el espacio de red del cliente. Y esos ataques no solo se dirigen a la capa 3, sino también a la capa 7 al mismo tiempo. Además, los ataques contra el sistema de nombres de dominio (DNS) han aumentado drásticamente y el grueso son ataques de consulta válida que pueden sobrecargar fácilmente la infraestructura de DNS del cliente. Solo unos pocos megabits de tráfico de DNS no deseado pueden causar una presión significativa en una empresa. También estamos empezando a ver un preocupante resurgimiento de la actividad de Mirai, que cobró una gran notoriedad por aprovechar la potencia del Internet de las cosas para causar interrupciones a gran escala.

En el panorama de amenazas actual, no basta con reforzar el borde de Internet para seguir el ritmo de los ataques. Las organizaciones necesitan un servicio de seguridad sólido a nivel de nube para asumir esa carga de trabajo y que les permita mantener la situación bajo control e implementar protecciones únicas para cada uno de esos terminales. Aquí es donde Akamai sobresale, tanto desde el punto de vista de la plataforma como de los servicios. Podemos aplicar varias capas de seguridad para defendernos de todo el espectro de los ciberataques. Asimismo, nuestros expertos cuentan con una amplia experiencia práctica que les permite examinar los matices y las tendencias de cada cliente. De este modo, la supervisión y la mitigación se efectúan de una forma muy concreta que bloquea las amenazas, pero deja pasar, al mismo tiempo, el tráfico previsto y limpio.

> El SOCC de Akamai nunca ha estado tan ocupado: a finales de 2023, habremos gestionado aproximadamente un 30 % más de tickets relacionados con la seguridad que el año pasado.
>
> **– Roger Barranco, Vicepresidente de Operaciones Globales de Seguridad, Akamai**

La batalla contra los bots puede ser brutal

Es complicadísimo mitigar el abuso de credenciales, ya que distinguir el tráfico no deseado del deseado es difícil y los clientes tienen back-ends relativamente únicos que pueden requerir soluciones de mitigación muy distintas. Además, los que efectúan este tipo de ataques se encuentran entre los más hábiles y atentos, ya que el abuso de credenciales es la forma más sencilla de obtener beneficios. Debido a la naturaleza peligrosa y costosa de estos ataques de bots, es importante contar con una solución de prevención del abuso de credenciales, sobre todo en los sectores de los servicios financieros y el comercio, donde el uso de bots maliciosos sigue aumentando.

EMEA sigue en el punto de mira de los atacantes

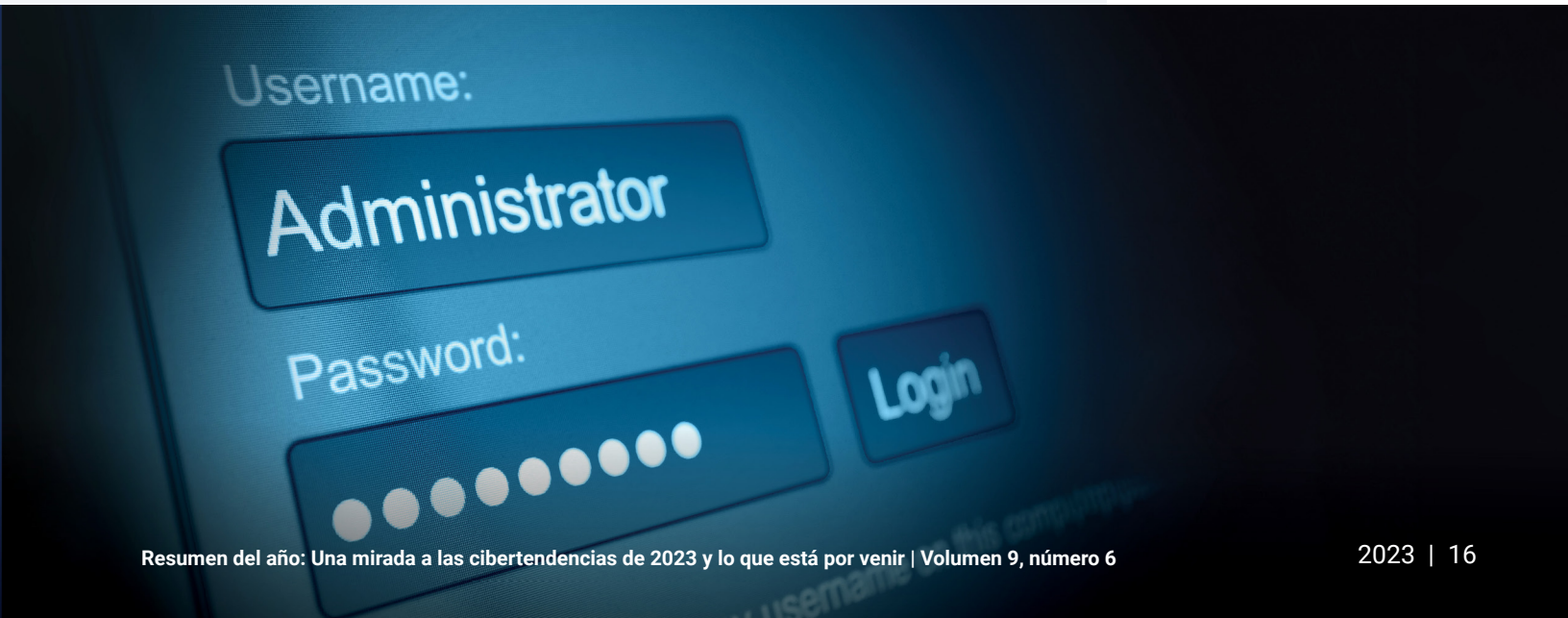
Desde la incursión en Ucrania, EMEA (Europa, en particular) ha desplazado a Estados Unidos como la principal región objeto de ciberataques en varios sectores y categorías de ataque, especialmente DDoS. Este cambio pone de relieve el hecho de que muchos agresores son Estados nación o simpatizantes de Estados nación, y su énfasis en Europa no disminuye.

La sofisticación de los atacantes va en aumento

Atrás quedaron los días en los que los "script kiddies" suponían la principal amenaza al utilizar herramientas genéricas para lanzar un ataque con la esperanza de tener suerte, o al alquilar una botnet DDoS por 10 dólares la hora para dejar fuera de combate a un adversario de un videojuego. Hoy en día, los atacantes son más sofisticados y parecen centrarse en objetivos concretos de forma detallada, planificar su estrategia, realizar reconocimientos a veces con un año de antelación y crear ataques para aprovechar posibles debilidades percibidas. A consecuencia de todo el trabajo preparatorio que efectúan los agresores, los ataques actuales son más prolongados que los de los últimos años, que a menudo solo duraban unos minutos.

A consecuencia de todo el trabajo preparatorio que efectúan los agresores, los ataques actuales son más prolongados que los de los últimos años, que a menudo solo duraban unos minutos.

– Roger Barranco,
Vicepresidente de Operaciones Globales de Seguridad,
Akamai



Prácticas recomendadas para la coordinación operativa y cibernética

A pesar de estos desafíos, los clientes pueden mejorar la eficacia de sus medidas de protección siguiendo dos prácticas recomendadas para la coordinación cibernética y operativa que permiten a Akamai trabajar como una extensión de su equipo cibernético. En primer lugar, deben colaborar con el SOCC en tiempos de paz para desarrollar de forma proactiva su estrategia de defensa, en lugar de intentar hacerlo durante un ataque. De esta forma, los ataques se pueden mitigar previamente, sin que la producción se vea afectada, y los clientes recibirán un informe de seguimiento que detalla el ataque evitado.

En segundo lugar, deben trabajar de forma proactiva en la capacidad operativa y los planes alternativos. Por ejemplo, deben asegurarse de que saben cómo habilitar e inhabilitar el acceso a distintas plataformas durante las pruebas. Un ataque de cinco minutos puede perjudicar a un cliente durante una hora debido a problemas operativos, por lo que estar preparado en materia de operaciones es tan importante como estar preparado para responder a un problema cibernético puro.

Este año ha puesto de relieve cómo la ciberseguridad cambia constantemente y esperamos que esta tendencia continúe. La buena noticia es que, al poner en práctica esta información, los clientes pueden ir un paso por delante y protegerse en 2024.

Momentos eureka y mucho más de nuestro director asesor de Seguridad de la Información

Me llamo Steve Winterfeld y soy el director asesor de Seguridad de la Información (CISO) de Akamai. Ocupé el puesto de CISO en Nordstrom Bank y de director de Respuesta a Incidentes e Inteligencia contra Amenazas en Charles Schwab. Me encargo de garantizar que nuestros partners tengan éxito a la hora de defender a sus clientes, así como de determinar dónde debemos centrar nuestros recursos.

Este año hemos visto algunas tendencias que me han sorprendido y otras que han quedado confirmadas por datos que pueden servir para actualizar nuestra estrategia. Las que considero las nueve historias más destacadas de este año incluyen momentos eureka, noticias esperadas y cosas que parece que nunca cambian.

Momentos eureka

- Entre el 10 % y el 16 % de las organizaciones ha detectado tráfico de mando y control (C2) en sus redes al menos una vez por trimestre. Además, el 26 % de los dispositivos infectados ha llegado a dominios relacionados con un agente de acceso inicial.
- El panorama de amenazas de ransomware ha experimentado un cambio preocupante en las técnicas de ataque, con el abuso desenfrenado de vulnerabilidades de día cero y de primer día en los últimos seis meses.
- La investigación de Akamai reveló que las víctimas de diferentes grupos de ransomware tienen casi seis veces más probabilidades de sufrir otro ataque durante los tres primeros meses posteriores al ataque inicial.

Noticias esperadas

- Los ataques dirigidos a la lógica empresarial de las API son difíciles de detectar y mitigar. En consecuencia, es difícil determinarlos en el nivel de solicitud individual.
- Las organizaciones deben garantizar el cumplimiento de los nuevos requisitos del estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS) v4.0 y el reglamento sobre la resiliencia operativa digital (DORA).

> Toda esta información constituye una guía excelente para mejorar su programa de seguridad y ver dónde tiene herramientas redundantes o carencias.
>
> **– Steve Winterfeld, Director asesor de Seguridad de la Información (CISO), Akamai**

Cosas que parece que nunca cambian

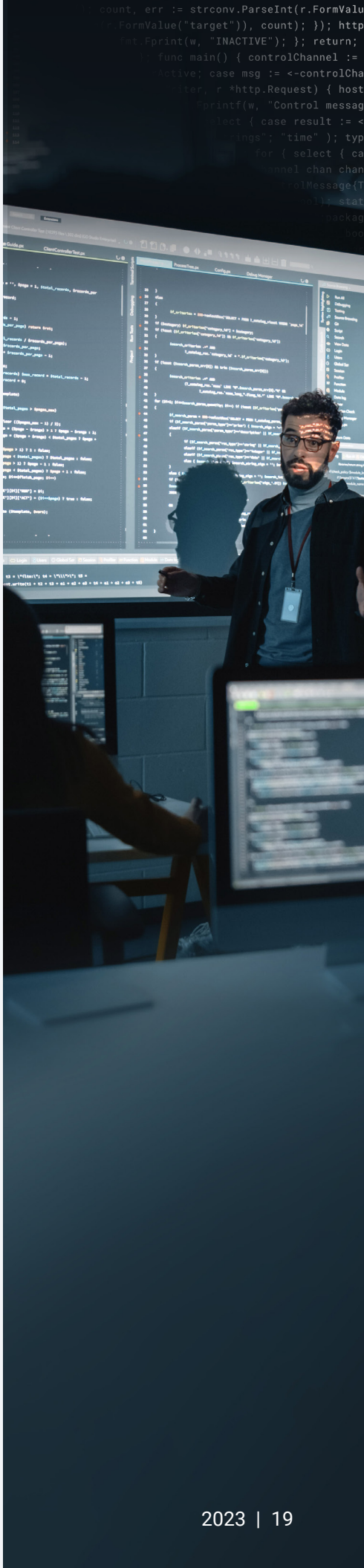
- Las cifras de los ataques de bots y API siguen creciendo y se están marcando nuevos récords de ataques DDoS.
- Los sectores más atacados suelen ser los servicios financieros, la alta tecnología y el comercio.
- La inclusión local de archivos (LFI) es la técnica de ataque más utilizada.
- Se está produciendo un cambio de Norteamérica a Europa como la región con más ataques DDoS.

Un descubrimiento fundamental que me dio que pensar fueron los indicadores de riesgo validados de la comunicación de C2. Lo que me resultó especialmente inquietante fue la alta frecuencia de detección inicial después de que el malware ya hubiera comprometido los sistemas y estuviera estableciendo la comunicación. Esto subraya la necesidad fundamental de equilibrar las medidas preventivas y la detección rápida para reducir al mínimo el impacto.

La historia que más me sorprendió fue el paso de los ataques a personas a través de la ingeniería social al uso de los ataques de día cero. Durante los últimos años, he tenido la sensación de que nuestras defensas técnicas se estaban fortaleciendo y de que tenía que reforzar al personal con formación y monitoreo. Sin embargo, tras el cambio de este año a los ataques de día cero, tengo que analizar detenidamente dónde voy a desplegar los recursos el año que viene.

Los ataques que parecen más injustos son los que se producen mientras una organización ya se está enfrentando a un ataque de ransomware o se está recuperando de un ataque de este tipo.
Es fácil centrarse demasiado en la crisis y sacar recursos de la supervisión defensiva continua. Esta investigación sirve para recordarle que no puede permitirse bajar la guardia.

Toda esta información constituye una guía excelente para mejorar su programa de seguridad y ver dónde tiene herramientas redundantes o carencias. Puede utilizarse como fundamento para los ejercicios para actualizar las guías y los procesos, dirigir la formación, mejorar los planes de pruebas de penetración o respaldar las revisiones de la cartera de riesgos. La ciberseguridad es un deporte de equipo, por lo que esta información también es útil para guiar las conversaciones con los partners internos (como los equipos jurídicos o de TI) y los proveedores. Como siempre, las referencias y herramientas como el Instituto Nacional de Normas y Tecnología (NIST), la base de conocimientos de MITRE ATT&CK y las 10 principales vulnerabilidades según OWASP son recursos excelentes.



Mirando hacia el futuro

Es imposible predecir el futuro, pero podemos prever que los ataques DDoS y a las API dominarán en 2024. Los continuos esfuerzos por generar ejércitos de botnets más grandes y desarrollar nuevas técnicas, junto con la influencia de los Estados nación, harán que los ataques DDoS aumenten. Este factor, junto con la evolución del ransomware, será la génesis de la legislación y la resiliencia.

La transformación sigue siendo el motor para la implementación de API en la mayoría de los sectores. Este rápido crecimiento conducirá de forma involuntaria a mayores superficies de ataque y más vulnerabilidades, API en la sombra, API zombis y abusos a las API. Prevemos un crecimiento significativo de los ataques contra aplicaciones web y API. Esto se debe tanto a ataques estándar, como LFI, como a técnicas emergentes, como la falsificación de solicitudes del lado del servidor (SSRF) y la inyección de plantillas del lado del servidor (SSTI), que requerirán herramientas capaces de detectar el movimiento lateral y mitigar los efectos.

Por último, con la excepción de algunas tendencias específicas del sector y la región, prevemos una escasez general de profesionales de ciberseguridad especializados. El aprendizaje automático y la inteligencia artificial de modelos de lenguaje de gran tamaño supondrán una cierta ayuda, pero en general será extremadamente difícil encontrar y retener el talento que necesitamos. Esto dará lugar a la colaboración con proveedores de dotación de personal a petición o servicios gestionados para puestos no esenciales.

En cuanto al SIG de Akamai, seguiremos dando la voz de alarma ante las amenazas prevalentes y los riesgos de seguridad emergentes que se vislumbren en el horizonte. Estaremos en contacto con la comunidad de seguridad a través de nuestras plataformas y nuestros canales para reforzar las iniciativas de inteligencia sobre amenazas. Y en 2024 celebraremos el décimo aniversario de nuestros informes SOTI. Estamos deseando seguir mejorando nuestros informes mediante la introducción de nuevos conjuntos de datos, ayudas visuales e información clave que puedan ayudar a los profesionales de la seguridad en su misión de mantener protegidas a sus organizaciones.

Esperamos compartir más información de investigación el año que viene. Mientras tanto, ¡protéjase!

Créditos

Editorial y redacción

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

Revisión y expertos en la materia

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Análisis de datos

Chelsea Tuttle

Marketing y publicación

Georgina Morales Hampe
Emily Spinks

Más información sobre el estado de Internet en materia de seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai y entérese de cuándo se publican los siguientes números. **akamai.com/soti**

Más información acerca de la investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad. **akamai.com/security-research**

Acceda a los datos de este informe

Vea versiones de alta calidad de los gráficos a los que se hace referencia en este informe. Puede usar estas imágenes y hacer referencia a ellas libremente, siempre que se cite debidamente a Akamai como fuente y que se conserve el logotipo de Akamai. **akamai.com/sotidata**

Más información sobre las soluciones de Akamai

Si desea obtener más información sobre las soluciones de Akamai contra amenazas, visite nuestra **página de soluciones de seguridad**.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com/ y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado en noviembre de 2023.