volumen 5, número 6

[Estado de Internet] / Seguridad

Resumen anual

Tabla de contenido

Carta del editor

Martin McKeay
Director editorial

Ha llegado el momento de hacer balance de este año 2019 que termina, y queremos aprovechar la oportunidad para agradecer a nuestros lectores su apoyo continuo al informe sobre el estado de Internet en materia de seguridad (SOTI) de Akamai. Tanto el equipo como el informe han evolucionado significativamente este año, y tenemos la intención de seguir creciendo y evolucionando en los años venideros. Nuestro objetivo es convertirnos en el informe de referencia al que acudir a la hora de afrontar una investigación importante.

¿Por qué Akamai elabora el informe SOTI y desarrolla investigaciones sobre seguridad en general?

A nivel interno, el informe SOTI y su investigación constituyen unos materiales excelentes de marketing. Una buena investigación posibilita crear buenas historias, que permiten dar a conocer lo que una empresa considera importante. En cierto modo, a la hora de labrarse su reputación, el tipo de investigación que cualquier empresa de seguridad publica es casi tan importante como el tipo de productos que vende.

¿Por qué un grupo global de investigadores defiende el valor de la investigación y la publicación? La mayoría de las respuestas individuales que hemos recibido se pueden reducir a dos motivos: el primero es que a todos, sin excepción, nos gusta que se nos reconozca como líderes y expertos en nuestro campo; y el segundo se refiere a la importancia del trabajo que desempeñan nuestros equipos. La investigación sobre seguridad es todavía un campo relativamente nuevo, por lo que cada dato, cada perla de sabiduría que contribuya al conocimiento global son valiosos.

Para mi equipo, que conforman los redactores, especialistas en datos y editores que elaboran este informe y mucho más, nuestro trabajo es nuestra pasión. Juntos, sumamos más de cuatro décadas de experiencia en el campo de la seguridad. Somos conscientes de todo lo que nos queda por descubrir y que apenas se cuantifica una pequeña parte de esos futuros descubrimientos. El hecho de trabajar con nuestros investigadores nos permite marcar la diferencia, al presentar su trabajo de manera que resulte atractiva e interesante a los lectores.

En un principio, el informe SOTI abordaba únicamente los ataques DDoS y a aplicaciones web, pero lo hemos ampliado para cubrir una amplia gama de los problemas de seguridad más importantes. Conforme Akamai evolucione como empresa de seguridad, los tipos de datos a nuestra disposición no harán más que aumentar. Ya hemos empezado a diseñar todo tipo de planes para el año 2020.

Los lectores son muy importantes para nosotros, ya que sin ellos este informe no existiría. Por este motivo, nos gustaría agradecerle su apoyo. Esperamos que, en 2020, nuestros informes le sigan resultando útiles. Por último, estaremos encantados de recibir cualquier comentario y pregunta que pueda tener.

La investigación de Akamai en 12 meses

Historias importantes de los últimos 12 meses

Le damos la bienvenida al sexto informe sobre el estado de Internet en materia de seguridad (SOTI) del año. A medida que se acerca el final de 2019, queremos hacer un balance retrospectivo y analizar la investigación que Akamai ha desarrollado en los últimos 12 meses. En este informe, que abarca el periodo desde principios de octubre de 2018 hasta finales de septiembre de 2019, prestaremos especial atención a la investigación realizada en el seno del equipo de respuesta a incidentes e inteligencia en seguridad (SIRT) de Akamai. Además, recopilaremos una selección de las noticias más importantes relativas al sector de la seguridad en el último año.

Aunque pueda parecer un cliché, este ha sido un año realmente interesante. Ahora más que nunca, las historias sobre seguridad adquieren cada vez más relevancia y empiezan a copar los titulares de las noticias en los medios de comunicación. Con las elecciones en la mente de la mayoría de personas en Estados Unidos, esperamos que la seguridad desempeñe un papel aún más decisivo, si cabe, en el próximo año.

Octubre de 2018

¡Menudo mes! Comenzó con una filtración de datos que afectó a millones de usuarios de Facebook. Unos días más tarde, Bloomberg publicó una noticia acerca de ataques informáticos a cadenas de suministro estatales y nacionales de EE. UU. Todos los proveedores mencionados en la noticia, así como el Departamento de Seguridad Nacional de EE. UU., negaron los hechos, pero Bloomberg se mantuvo firme en la veracidad de sus informes.

Octubre fue también un mes ajetreado para nuestros equipos de seguridad. Ryan Barnett, de Akamai, publicó una entrada en el blog sobre los encabezados de respuesta de seguridad y por qué los responsables empresariales y los de seguridad deberían preocuparse por ellos. Un día después, Larry Cashdollar publicó un análisis del kit de phishing Luis que incluía algunas de sus técnicas de evasión.

Larry Cashdollar también informó sobre la vulnerabilidad de carga de archivos jQuery (CVE-2018-9206). Aunque el problema se solucionó, las bifurcaciones y la reutilización del código se extendieron a otros códigos base, con la consiguiente posibilidad de afectar a 7800 proyectos. En una entrada de seguimiento, Larry Cashdollar realizó pruebas en 1000 proyectos bifurcados con el código jQuery y descubrió que 970 de ellos eran vulnerables.

Con las elecciones en la mente de la mayoría de personas en Estados Unidos, esperamos que la seguridad desempeñe un papel aún más decisivo, si cabe, en el próximo año.

Noviembre de 2018

El mes de noviembre se estrenó con la noticia de que la Biblioteca del Congreso y la Oficina de Derechos de Autor de EE. UU. habían añadido excepciones a la Ley de Derechos de Autor para Medios Digitales en el Nuevo Milenio estadounidense (DMCA). Una de esas exenciones permite a los investigadores exponer defectos de software sin temor a persecuciones legales. A esta noticia le siguió la publicación de informes según los cuales alrededor de 60 millones de tarjetas de pago estadounidenses se habían visto comprometidas entre 2017 y 2018; el 93 % eran tarjetas de pago EMV.

En esos días, Kaan Onarlioglu, de Akamai, publicó una entrada en el blog en la que abordaba las evaluaciones de vulnerabilidad de terceros de Akamai Intelligent Edge Platform, así como la existencia de falsos positivos que pueden generar confusión. Poco después, Ryan Barnett publicó un exhaustivo informe sobre las medidas que se deben tomar para protegerse de los ataques de Magecart. Por otra parte, Or Katz elaboró un análisis detallado de una estafa de phishing con 78 variaciones diferentes. Con el año 2019 a punto de terminar, el software Magecart sigue siendo una amenaza importante, en gran parte debido a las vulnerabilidades del software y los complementos de terceros que aún se emplean en muchos sitios.

Diciembre de 2018/enero de 2019

A finales de 2018, los equipos de publicación e investigación también dieron los últimos retoques al primer informe sobre el estado de Internet en materia de seguridad de 2019, publicado el 30 de enero. Los investigadores, e incluso los hackers, se tomaron buena parte de diciembre de vacaciones.

Antes de publicar el informe SOTI, Larry Cashdollar publicó una entrada sobre la vulnerabilidad ThinkPHP (CVE-2018-20062), que descubrió mientras investigaba los ataques de clonación de tarjetas de Magecart. En una entrada posterior, Lukasz Orzechowski compartió un experimento con herramientas de traducción asistida por ordenador (CAT). La traducción de un idioma a otro no es tarea sencilla, y se complica aún más cuando nos encontramos ante un script informático con un lenguaje técnico.

Estado de Internet / Seguridad: volumen 5, número 1

Ataques DDoS y contra aplicaciones web

En este número, abordamos la salud mental, con un ensayo de la autora invitada Amanda Berlin. Desde enero, el número de talleres que la asociación Mental Health Hackers ha organizado en conferencias de seguridad ha crecido en Estados Unidos.

Profundizamos en un incidente que, a primera vista, parecía un ataque DDoS masivo, con más de 4000 millones de solicitudes en más de 15 582 direcciones IP. Sin embargo, el supuesto ataque resultó deberse a una serie de errores en una aplicación.

También tratamos el tema de los bots en el sector del retail y cómo las aplicaciones All-in-One (AIO) pueden tener un gran impacto en las ventas y promociones online. Aunque no todos los bots son malos, sin duda algunos pueden causar más problemas de los que deberían.

En resumen

- Los problemas de salud mental cuestan a las empresas estadounidenses más **de 190 000 millones de dólares** al año en pérdidas de beneficios.
- A veces, un "ataque" no es exactamente lo que parece a primera vista. Los expertos del centro de control de operaciones de seguridad (SOCC) de Akamai observaron el impacto de **4000 millones de solicitudes** en un importante sitio web y profundizaron en la causa real.
- **Los bots reportan importantes beneficios económicos a los atacantes**, que se aseguran de actualizarlos constantemente para eludir las nuevas defensas que vayan surgiendo. Un atacante ofreció 15 000 dólares en su búsqueda de desarrolladores con experiencia en ataques dirigidos a defensas de empresas específicas.

Febrero de 2019

El frío de febrero caló en el flujo de noticias. Sin embargo, hubo algunas historias candentes, como el caso en el que una persona presentó una demanda judicial contra Apple por forzar la autenticación de dos factores en las cuentas de usuario.

También fue noticia una carta de notificación de incidentes presentada ante la Oficina del Fiscal General de Vermont (PDF). El incidente en cuestión era un ataque de Credential Stuffing dirigido a los usuarios de TurboTax, más que una filtración de los sistemas Intuit. Ejemplos como este son una de las razones por las que Akamai siguió la pista a la autenticación multifactorial y al Credential Stuffing a lo largo de 2019. Otra razón es el gran volumen de ataques de Credential Stuffing que, a día de hoy, Akamai sigue identificando.

Justo antes de que se publicara el segundo número del informe SOTI en febrero, Larry Cashdollar escribió una entrada en el blog en la que analizaba el uso de Google Translate en ataques de phishing contra Facebook. Consejo: no provoque con intentos de phishing a investigadores que se ganan la vida profundizando en patrones extraños e inusuales.

Akamai siguió la pista a la autenticación multifactorial y al Credential Stuffing a lo largo de 2019.

Estado de Internet / Seguridad: volumen 5, número 2

Tráfico de API y ataques al sector de retail

Esta fue la primera vez del año que Akamai analizó a fondo los datos de Credential Stuffing. Cuando se publicó este informe, Akamai había observado 10 000 millones de intentos de Credential Stuffing en el sector del retail entre mayo y diciembre de 2018. El informe también ahondó en los bots de AIO en el sector del retail, la seguridad de las API y los posibles problemas de IPv6.

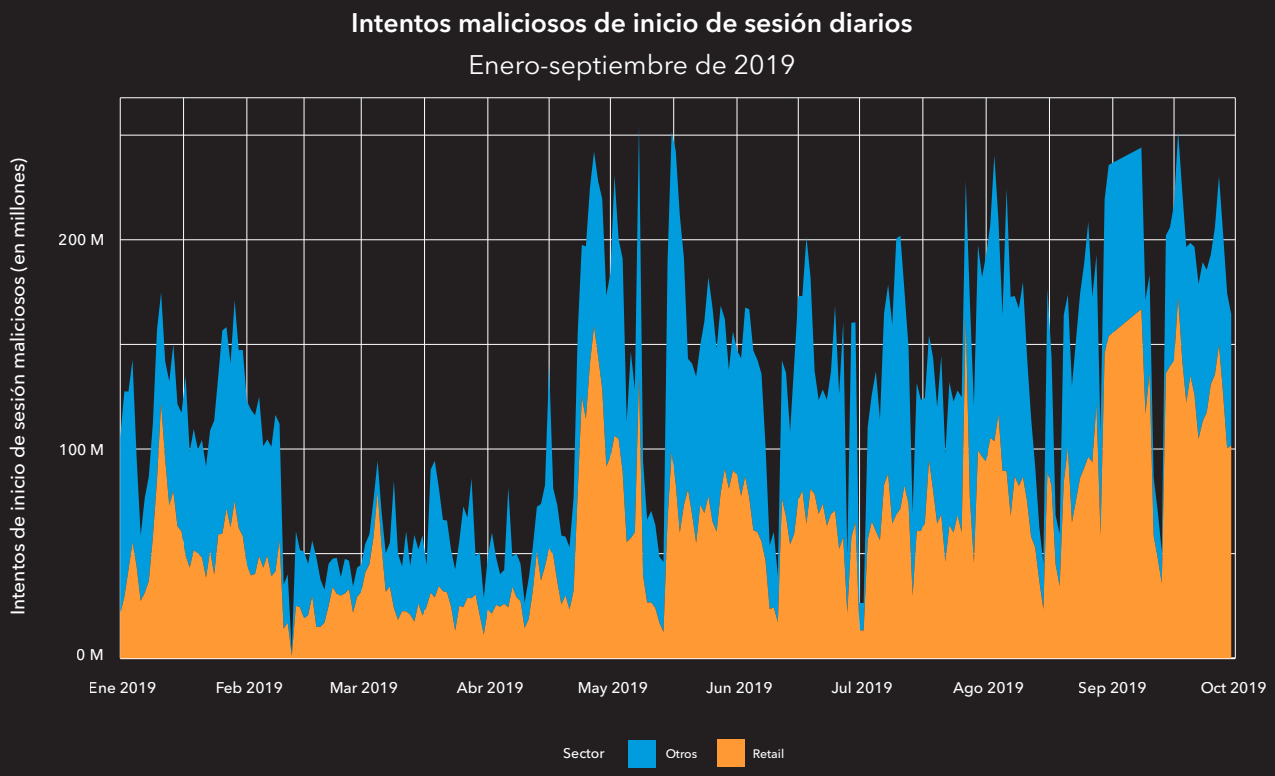


Fig. 1. Actualización del gráfico publicado en el informe número 2. El Credential Stuffing sigue teniendo como objetivo principal al sector del retail con 16 500 millones de intentos entre enero y septiembre de 2019; en 2018, el número de intentos entre abril y diciembre fue de 11 500 millones.

En resumen

- Akamai detectó casi 28 000 millones de ataques de Credential Stuffing entre mayo y diciembre de 2018 en todos los sectores (no solo el de retail).
- Según el análisis de Akamai, el uso de IPv6 podría estar infravalorado, lo que presupone de forma temeraria que no merece la pena supervisar el tráfico IPv6.
- Un análisis de la red ESSL de Akamai reveló una división entre el tráfico de API (que representa el 83 %) y de HTML (que supone el 17 %) en nuestra red de distribución de contenido (CDN) segura. Se trata de un aumento significativo desde que se realizara la misma encuesta en 2014.

Marzo de 2019

Al abordar los intentos de Credential Stuffing, uno de los temas clave es el uso de contraseñas fáciles de adivinar o débiles. Además, existe un gran número de usuarios que recicla sus contraseñas en varias redes y servicios. A principios de marzo, salieron a la luz algunas historias sobre el servicio de telefonía Xfinity Mobile de Comcast con el código 0000 como PIN predeterminado en las cuentas de clientes. Esta historia circulaba poco después de que se supiera que la contraseña del iPhone X del rapero y empresario Kanye West era 000000.

Fuera del flujo de noticias, Jonathan Respeto, de Akamai, publicó una entrada sobre el uso de los programas Capture the Flag para promover la formación continua en el centro de control de operaciones de seguridad (SOCC).

Abril de 2019

El mes de abril llegó de repente y, mientras el equipo se recuperaba del evento RSA Conference, la noticia de un trío de vulnerabilidades de día cero de WordPress comenzó a correr por las redes, lo que dio lugar a una serie de ataques al sitio web. Los investigadores de Akamai observan con frecuencia que los delincuentes utilizan sitios web vulnerables para alojar kits de phishing. Esto también es útil para la evasión, ya que es poco probable que un sitio web legítimo, pero vulnerable, levante sospechas o active las alarmas de defensa de punto final.

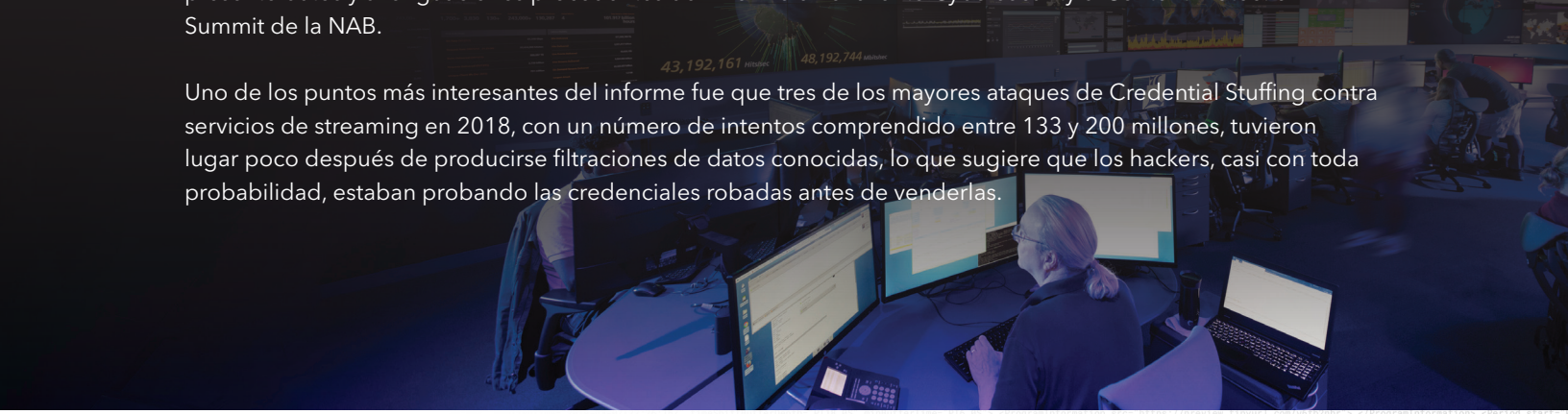
Siguiendo con el tema de las vulnerabilidades, Larry Cashdollar publicó una entrada de blog en la que advirtió sobre diversas vulnerabilidades en Magento. El aviso, publicado para llamar la atención sobre el tema, destacó más de 30 vulnerabilidades en la plataforma, incluida una en la que se estaba realizando una prueba de concepto en ese momento. Avanzado el mes, el investigador Yael Daihes, junto con Craig Sprosts, informó en el blog acerca de cómo aumentar la eficacia mediante la incorporación de datos DNS reales a modelos de aprendizaje profundo.

Estado de Internet / Seguridad: edición especial sobre el sector multimedia

Credential Stuffing: ataques y mercados

Esta edición especial del informe SOTI, que vio la luz el 8 de abril de 2019, se publicó pensando en los asistentes del sector multimedia a la conferencia de National Association of Broadcasters (NAB). Patrick Sullivan, de Akamai, presentó datos y averiguaciones procedentes del informe en el evento Cybersecurity & Content Protection Summit de la NAB.

Uno de los puntos más interesantes del informe fue que tres de los mayores ataques de Credential Stuffing contra servicios de streaming en 2018, con un número de intentos comprendido entre 133 y 200 millones, tuvieron lugar poco después de producirse filtraciones de datos conocidas, lo que sugiere que los hackers, casi con toda probabilidad, estaban probando las credenciales robadas antes de venderlas.



Mayo de 2019

Lo más destacado de mayo fueron los parches de Cisco para paliar las importantes vulnerabilidades de los routers y los problemas de ransomware de Baltimore, así como los esfuerzos de recuperación. El ransomware ha sido un tema recurrente en el último año y no parece que su uso vaya a menguar.

Amiram Cohen, de Akamai, junto con una investigación más exhaustiva de Or Katz, publicó un análisis detallado del kit de phishing 16Shop dirigido a los usuarios de Apple. El kit en sí es avanzado, se actualiza de forma constante y utiliza una serie de técnicas de evasión. Asimismo, el equipo de investigación de amenazas de Akamai escribió una entrada relacionada con la técnica Cipher Stunting, o cifrado retardado. Se trata de una amenaza creciente que genera firmas SSL/TLS de forma aleatoria en un intento de eludir los sistemas de detección.

Junio de 2019

En junio, las noticias de seguridad suelen copar la actualidad, y este año no fue una excepción. Se produjeron ataques contra los plugins de WordPress, filtraciones de datos e incidentes relacionados con malware dirigido a puntos de venta en 102 restaurantes Checkers y Rally's de 20 estados de EE. UU. También fueron noticia asuntos más mundanos como el que abordó un estudio según el cual el sesgo cognitivo afecta a las decisiones de seguridad.

Larry Cashdollar y Steve Ragan estrenaron el blog en junio con la identificación de vulnerabilidades en kits de phishing, las cuales, si se aprovechan, podrían suponer problemas añadidos para los administradores de servidores. Además de hacer una presentación en la conferencia Edge World de Akamai, Or Katz publicó un par de entradas relacionadas con técnicas de evasión de kits de phishing y análisis de phishing. Por su parte, Larry Cashdollar publicó dos entradas más ese mismo mes. En la primera, del 13 de junio, abordó 26 vectores de infección en la que por entonces era la versión más reciente de Echobot. A final del mes, escribió acerca de un bot llamado Silex que inutilizaba los sistemas, una vez infectados.

Estado de Internet / Seguridad: Volumen 5, número 3

Ataques web y abuso en videojuegos

Esta edición del informe SOTI se centra en los videojuegos y en la economía delictiva subyacente. Los videojuegos son un objetivo muy habitual, y los delincuentes disponen de varias maneras de dirigirse a los jugadores y a las empresas responsables de algunos de los videojuegos más populares de Internet. En lo que respecta a los datos, el informe señaló que hubo 12 000 millones de ataques de Credential Stuffing contra sitios web de videojuegos entre noviembre de 2017 y marzo de 2019. En el mismo periodo, se registraron más de 55 000 millones de ataques de Credential Stuffing en todos los sectores. Según el informe, las aplicaciones web también fueron un objetivo común, con predominio de los ataques de inyección SQL (SQLi), que representaron casi dos tercios del total de ataques dirigidos a aplicaciones web.

Ataques diarios a aplicaciones web

Enero-septiembre de 2019

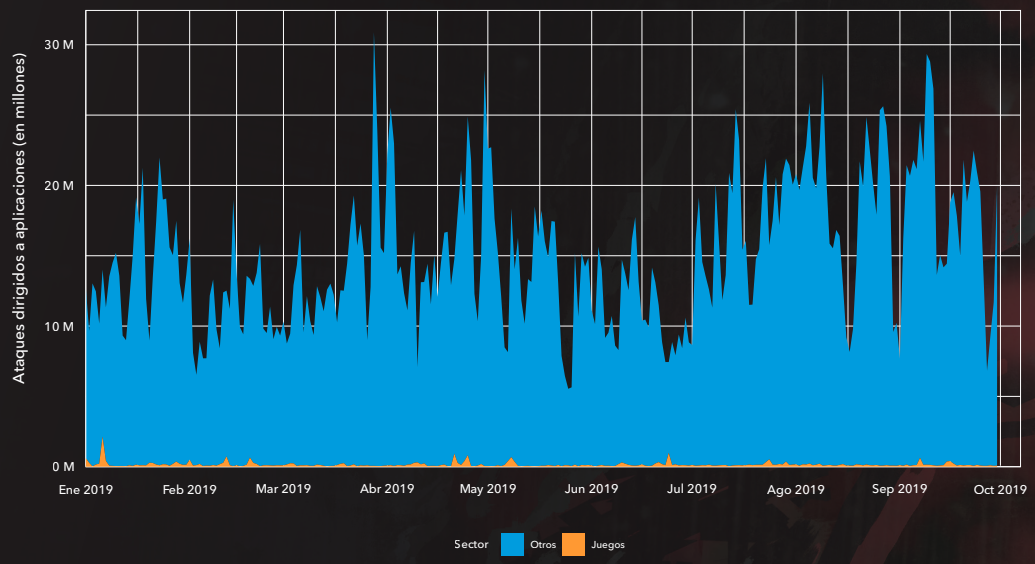


Fig. 2. Aunque las empresas de videojuegos solo sean el objetivo de un pequeño porcentaje de los ataques que observa Akamai, ya ha se han detectado más de 35 millones de intentos dirigidos a este sector entre enero y septiembre de 2019.

Ataques diarios a aplicaciones por vector

Enero-septiembre de 2019

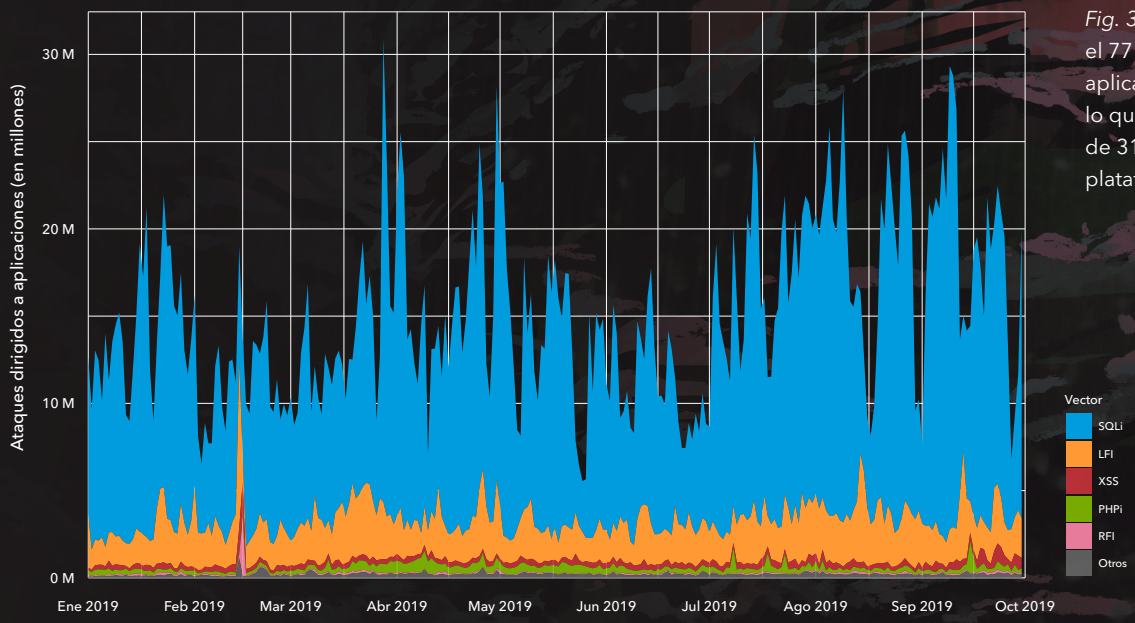


Fig. 3. Los ataques SQLi representan el 77 % de todos los ataques a aplicaciones hasta la fecha en 2019, lo que supone la generación de más de 3100 millones de alertas en la plataforma de Akamai.

En resumen

- Akamai observó 55 000 millones de ataques de Credential Stuffing a lo largo de 17 meses, de los cuales 12 000 millones estaban dirigidos directamente al sector de los videojuegos.
- Los ataques de SQLi son la principal amenaza en lo que respecta a riesgos de las aplicaciones web, ya que representan casi dos tercios de todos los ataques.
- En general, Estados Unidos sigue siendo la principal fuente de ataques de Credential Stuffing, seguida de Rusia. Sin embargo, si solo se tienen en cuenta los datos del sector de los videojuegos, Rusia ocupa el primer puesto.

Julio de 2019

En julio, la mayoría de las personas que trabajan en el sector de la seguridad, incluidos muchos de los empleados en Akamai, empezaron a prepararse para asistir a las conferencias previstas para agosto en Las Vegas. Las empresas de seguridad hablan mucho sobre riesgos y superficies de ataque. Una de las superficies de ataque más comunes es el navegador; por ello, la noticia de que la agencia alemana *Bundesamt für Sicherheit in der Informationstechnik* (BSI) preparaba el borrador de unas directrices para la seguridad del navegador no pasó desapercibida.

En el ámbito de la investigación interna, Chad Seaman, de Akamai, publicó una entrada sobre los ataques SYN-ACK. Lior Lahav y Asaf Nadler analizaron los últimos cambios en el algoritmo de generación de dominios (DGA) para Pykspa v2, seguido de una segunda entrada en la que ahondaron en las mitigaciones del DGA. Por último, el 29 de julio, Larry Cashdollar informó en el blog acerca de los delincuentes que aprovechan las vulnerabilidades de la inclusión remota de archivos (RFI) en sus campañas de phishing.

Estado de Internet / Seguridad: volumen 5, número 4

El mercado de los ataques al sector financiero

En esta edición del informe SOTI, analizamos cómo los ataques y las herramientas que se utilizan contra los servicios financieros forman parte de un ecosistema mayor y más complejo. El informe se adentra en los mercados delictivos y observa cómo estos dirigen sus ataques a instituciones financieras, así como lo que sucede después de que un ataque tenga éxito.

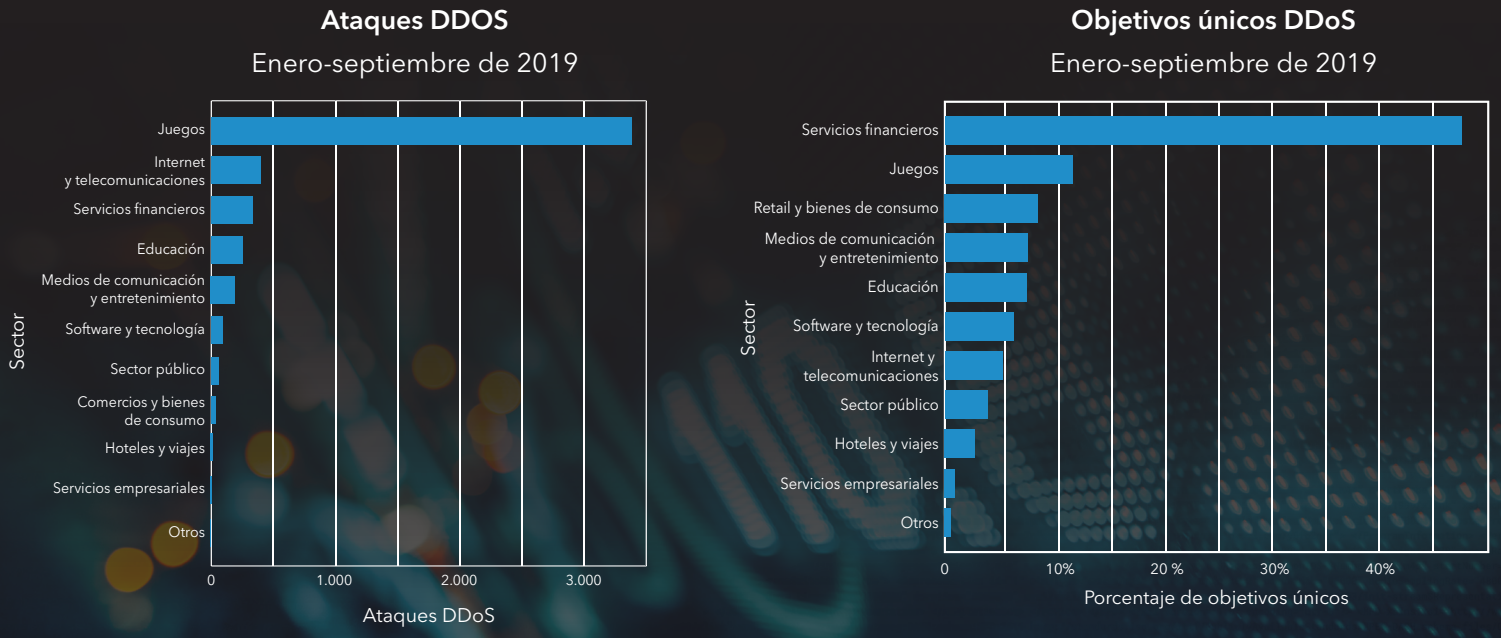


Fig. 4. Actualización del gráfico publicado en el informe número 4. Los ataques DDoS suelen dirigirse a empresas de videojuegos, pero los ataques contra el sector financiero están mucho más dispersos en múltiples objetivos.

En resumen

- La mitad de todas las entidades suplantadas por dominios de phishing pertenecían al sector financiero, según los datos de Akamai.
- Más del 6 % de los intentos de inicio de sesión maliciosos estaban dirigidos al sector financiero de forma global.
- El 94 % de los ataques contra el sector financiero procedían de ataques SQLi, LFI, secuencias de comandos en sitios cruzados (XSS) e inyecciones de OGNL mediante Java.

Agosto de 2019

A principios de agosto, se celebraron las conferencias de Black Hat, DEF CON y BSides Las Vegas. La mayor parte de los primeros titulares del mes se referían a lo que la periodista Violet Blue bautizó como la "temporada de ciberanzuelos de la seguridad de la información". Sin embargo, la noticia con más repercusión no tenía nada que ver con la seguridad: se trataba de un hombre con un televisor en la cabeza que fue grabado mientras dejaba televisores en los porches de Virginia. Después de evitar por los pelos una plaga de langostas en Las Vegas, los asistentes al evento Black Hat se enteraron de que todos aquellos que estuvieran en la zona entre el 3 y el 5 de agosto podrían haber estado expuestos al virus del sarampión.

En el departamento de investigación, Or Katz, de Akamai, publicó una entrada sobre estafas de phishing dirigidas a puntos de gran afluencia turística y Larry Cashdollar escribió sobre la propagación del software de minería de criptomonedas XMR.

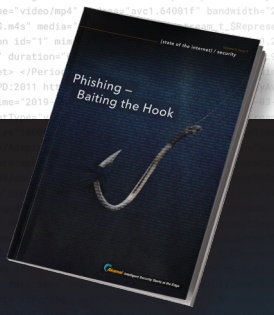
Septiembre de 2019

Jonathan Respeto y Chad Seaman, de Akamai, publicaron una entrada en la que analizaban un nuevo vector de DDoS que puede alcanzar los 35 Gbps. El vector, que aprovecha una técnica de amplificación UDP conocida como WS-Discovery (WSD), se puede utilizar para obtener unas tasas de amplificación de hasta el 15 300 %.

Estado de Internet / Seguridad: Edición especial sobre el sector multimedia

Medios de comunicación bajo ataque

Esta edición especial del informe SOTI, publicada con motivo de la feria de multimedia, entretenimiento y tecnología IBC, retomó el seguimiento de las actividades de Credential Stuffing con un análisis detallado acerca de cómo afectan a las empresas multimedia y tecnológicas. En total, entre enero de 2018 y junio de 2019, Akamai registró más de 61 000 millones de intentos de Credential Stuffing y más de 4000 millones de ataques dirigidos a aplicaciones web.



Estado de Internet / Seguridad: volumen 5, número 5

Phishing: cómo no caer en la trampa

El último informe de investigación SOTI del año se centró en el phishing y en el mercado y los métodos que lo sustentan. Este número también incluye, por primera vez, datos del seguimiento interno de Akamai sobre intentos de phishing dirigidos a nuestros empleados.

En resumen

- El 60 % de los kits de phishing vigilados por Akamai estuvieron activos durante 20 días, o incluso menos.
- El principal objetivo del phishing es el sector de la alta tecnología, según los datos de Akamai.
- Microsoft, PayPal, DHL, Dropbox, DocuSign y LinkedIn son los principales objetivos de phishing, según la supervisión de Akamai.

Fuentes de noticias

Además de las fuentes vinculadas en este informe, a continuación se incluye una lista con algunas fuentes de noticias que los colaboradores de este informe consultan asiduamente para obtener análisis útiles e información sobre el sector.

- Violet Blue
- Zack Whittaker
- Dark Reading
- Ars Technica
- Motherboard
- CyberScoop
- CSO Online
- WIRED
- TechCrunch
- ZDNet
- SecurityWeek
- Forbes

Una mirada hacia el futuro

Ha llegado la temporada de las "predicciones sobre seguridad" y, a decir verdad, no es algo que nos entusiasme.

Los futuristas y los autores de ciencia ficción realizan predicciones sobre el futuro. Gene Roddenberry y su universo de *Star Trek* se han convertido en un elemento básico de la conciencia colectiva y han predicho o promovido la creación de muchos de los aparatos que utilizamos a diario, como teléfonos móviles o auriculares Bluetooth. Sin embargo,

Ojalá viva tiempos interesantes.

Antigua maldición china

nosotros somos profesionales de la seguridad, no futuristas, y nunca hemos sido capaces de hacer predicciones precisas con un año de antelación.

Lo que sí podemos hacer es observar los datos que tenemos hoy y extrapolar las tendencias. Probablemente se esté preguntando que en qué se diferencia eso de una predicción. La respuesta a su hipotética pregunta es, principalmente, la perspectiva. Tanto la extrapolación como la predicción son intentos de encontrar tendencias emergentes, pero la predicción tiene un sesgo más subjetivo.

Cuando se le pide a alguien que haga una predicción, se supone que la respuesta debe ser novedosa y diferente a lo que otros ya han señalado; la extrapolación se basa más en las tendencias reales. Sí, esto de la extrapolación es hilar muy fino y hasta pretencioso, pero ese nivel de especificidad es lo que deberíamos esperar de los investigadores y los editores.

¿Qué podemos extrapolar de las tendencias de 2019? En primer lugar, se mantendrá el crecimiento del abuso de credenciales, el phishing y la explotación de vulnerabilidades en sistemas populares. Esta predicción es sencilla, pero la diferencia es que observamos una mayor complejidad y profesionalización de estos ataques. En cualquier caso, seremos testigos de ataques más complejos y heterogéneos.

Hace una década, los delincuentes eran quienes normalmente hallaban las vulnerabilidades para luego incorporarlas a los ataques. Hace cinco años, la norma eran los equipos de delincuentes profesionales que descubrían y desarrollaban software de ataque. Actualmente, la tendencia consiste en un solapamiento de desarrolladores delictivos y la amenaza persistente avanzada (APT), o actores a nivel nacional y estatal, por el que se genera un flujo constante de herramientas de día cero dirigidas a personas físicas y organizaciones concretas.

Esta no es una mera especulación. A principios de octubre, la NSA, en una reacción extrema, emitió una advertencia de que conocidos actores a nivel nacional y estatal estaban dirigiendo ataques a plataformas VPN vulnerables. Existen numerosos canales de comunicación alternativos desde los que se suelen emitir tales avisos, por lo que esta forma de proceder da muestras de que la NSA lo percibe como un peligro claro y real.

Empieza a quedar lejos la época en la que los asesores de seguridad de una empresa se consideraban alarmistas. En cambio, nos dirigimos a unos tiempos en los que, en ocasiones, la gravedad y el impacto de los ataques nos pillan desprevenidos hasta a nosotros. Los temas esotéricos sobre seguridad, que solían ser el terreno de especialistas y técnicos, ahora forman parte del flujo de noticias diario y de la conciencia colectiva. Muchas de las predicciones de hace una década se están materializando, y eso que las amenazas no se parecen en nada a lo que la mayoría de nosotros preveíamos.

Una predicción que sí nos atrevemos a hacer es que 2020 promete ser un año interesante.

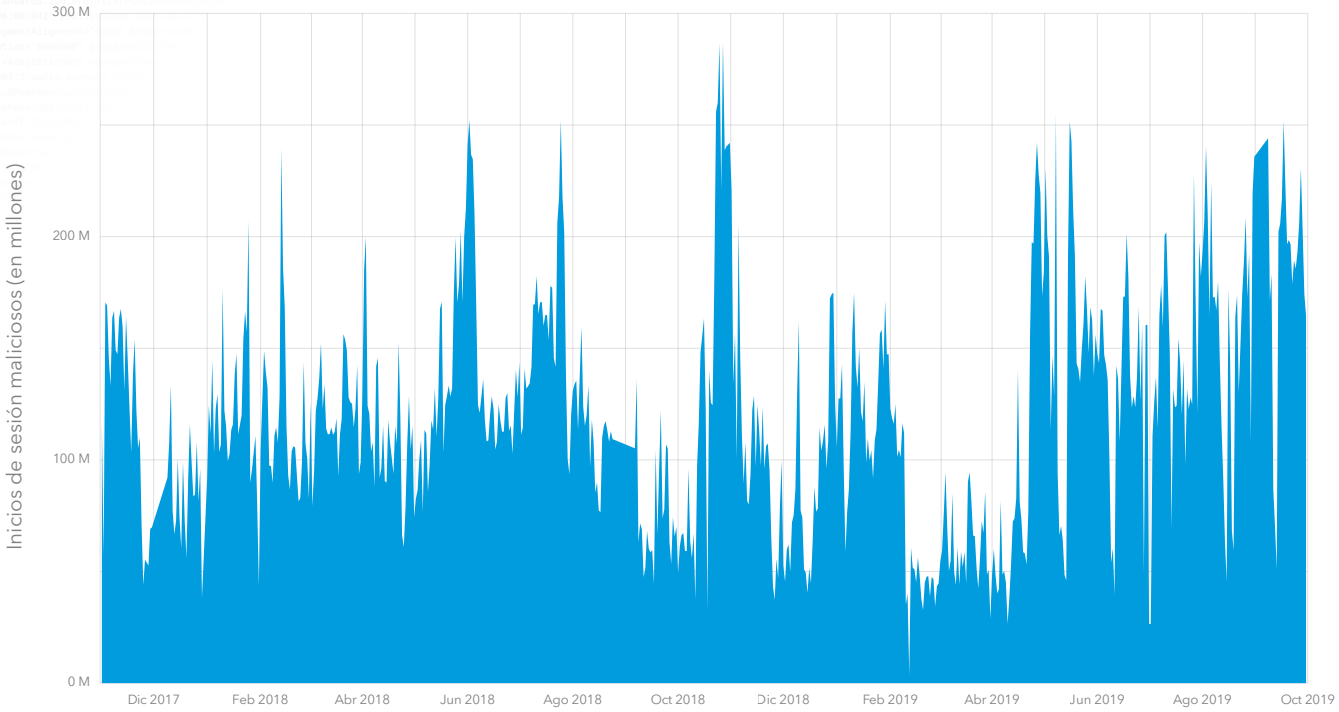
Apéndice

Actualizaciones importantes de nuestras grandes historias

Los siguientes gráficos son actualizaciones del trabajo de números anteriores del volumen 5 del informe sobre el estado de Internet en materia de seguridad. Las incluimos para los lectores a modo de información complementaria con una explicación y un texto de acompañamiento breves. Todos los gráficos y las tablas se refieren al periodo comprendido entre noviembre de 2017 y septiembre de 2019.

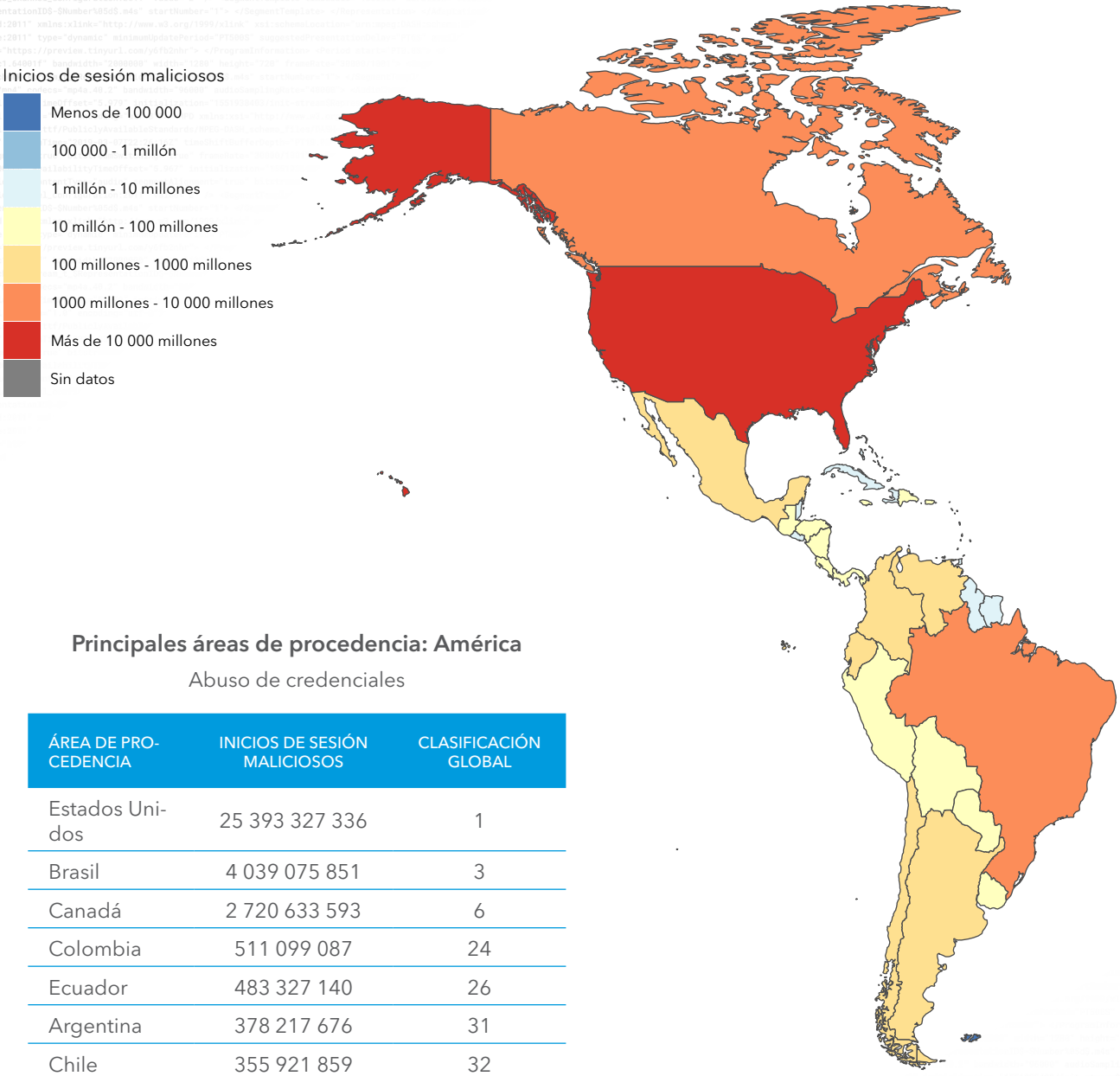
Intentos maliciosos de inicio de sesión diarios

Noviembre de 2017 – septiembre de 2019



Fuentes de ataques de abuso de credenciales: América

Noviembre de 2017 – septiembre de 2019



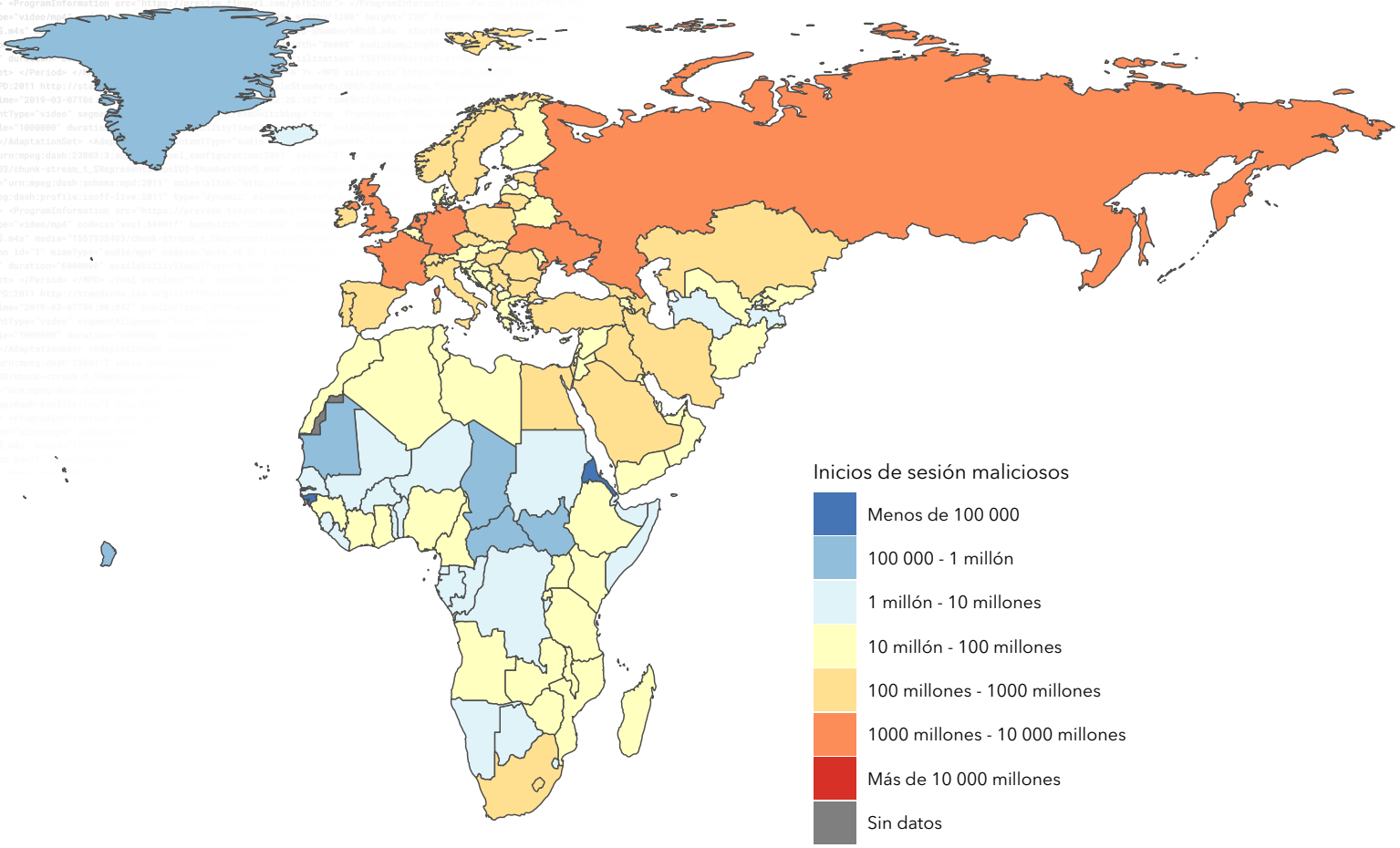
Principales áreas de procedencia: América

Abuso de credenciales

ÁREA DE PRO-CEDENCIA	INICIOS DE SESIÓN MALICIOSOS	CLASIFICACIÓN GLOBAL
Estados Uni-dos	25 393 327 336	1
Brasil	4 039 075 851	3
Canadá	2 720 633 593	6
Colombia	511 099 087	24
Ecuador	483 327 140	26
Argentina	378 217 676	31
Chile	355 921 859	32
México	344 094 629	34
Venezuela	177 795 687	47
Perú	90 149 099	65

Fuentes de ataques de abuso de credenciales: EMEA

Noviembre de 2017 – septiembre de 2019



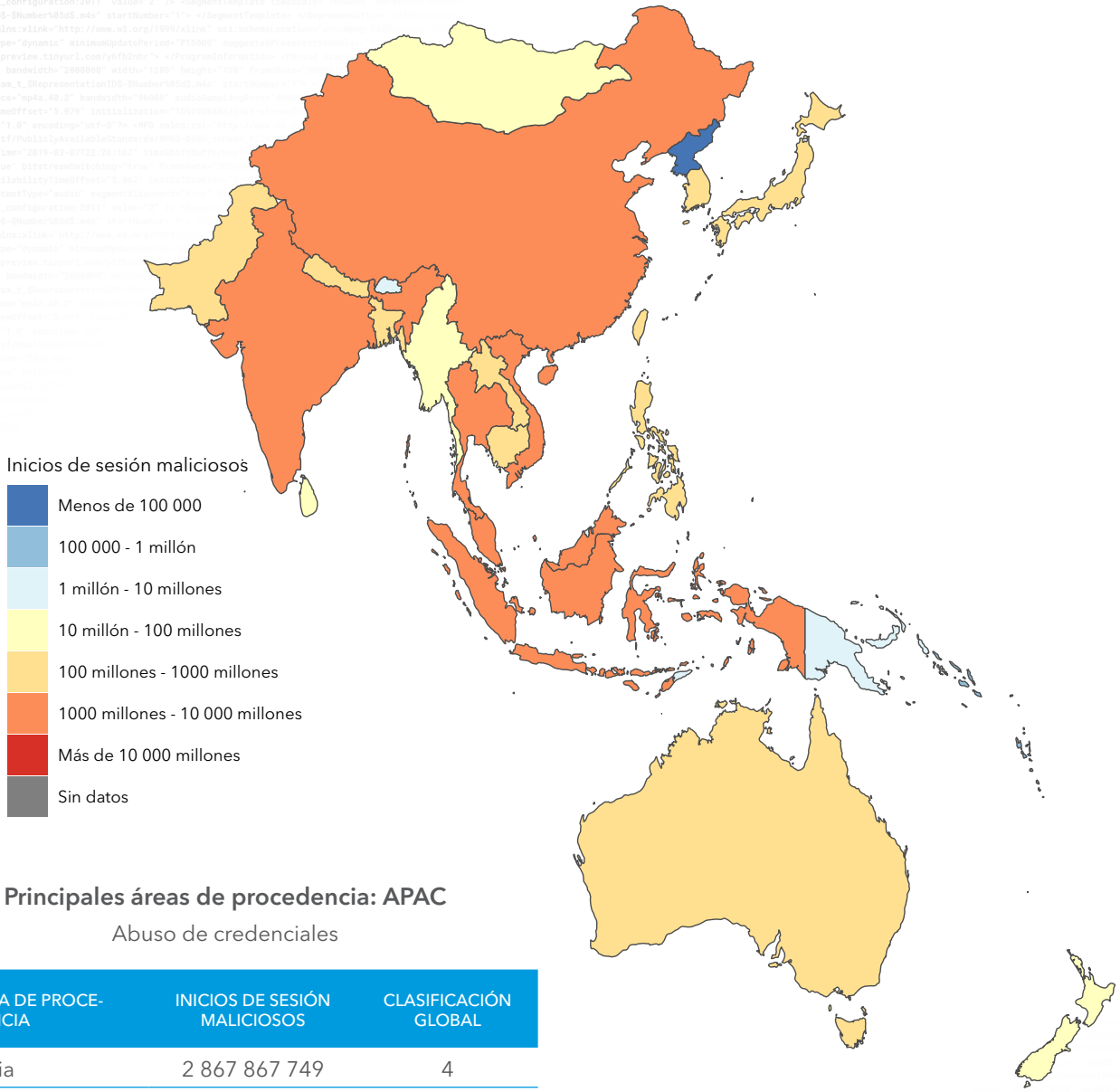
Principales áreas de procedencia: EMEA

Abuso de credenciales

ÁREA DE PROCEDENCIA	INICIOS DE SESIÓN MALICIOSOS	CLASIFICACIÓN GLOBAL
Rusia	6 114 186 048	2
Alemania	2 129 388 432	10
Francia	2 081 826 451	11
Países Bajos	1 723 393 319	12
Reino Unido	1 559 263 043	14
Ucrania	1 097 729 730	16
Italia	879 866 419	17
Estonia	652 938 763	21
Polonia	571 536 319	23
España	490 167 797	25

Fuentes de ataques de abuso de credenciales: APAC

Noviembre de 2017 – septiembre de 2019



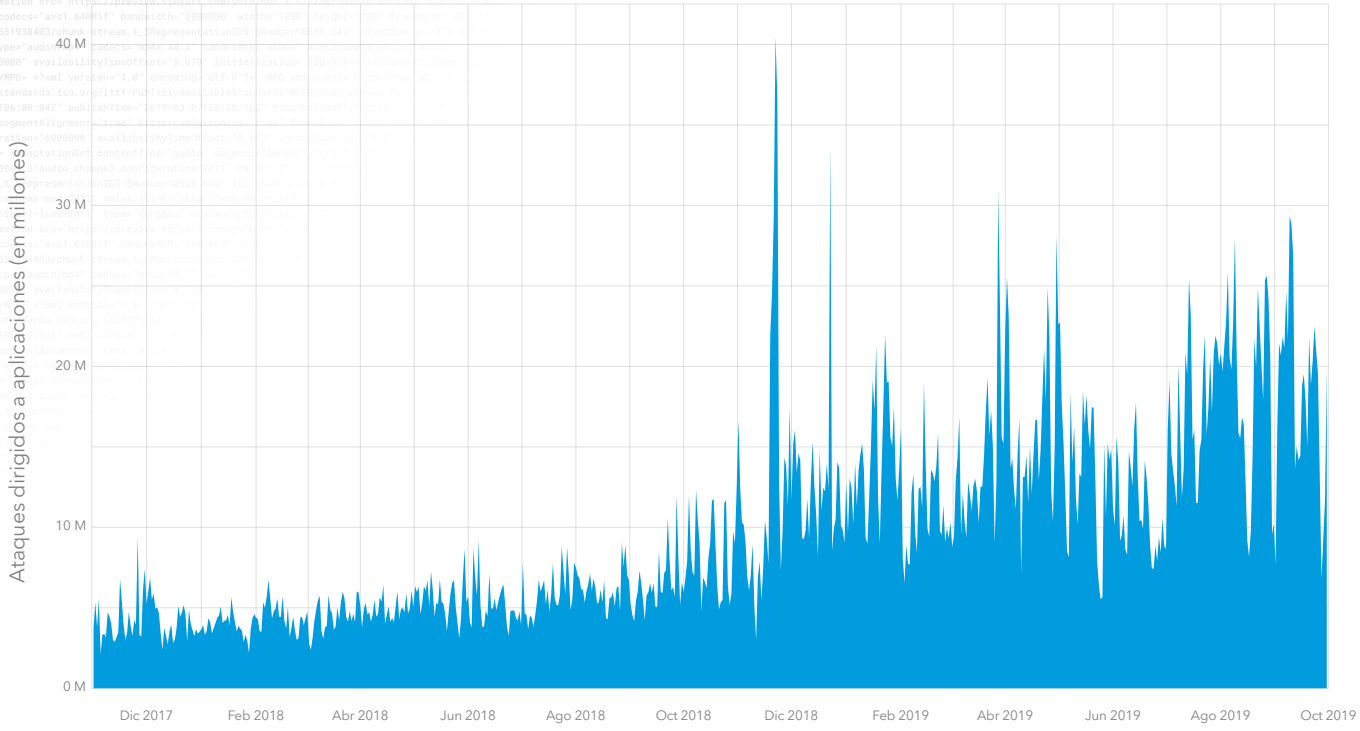
Principales áreas de procedencia: APAC

Abuso de credenciales

ÁREA DE PROCEDENCIA	INICIOS DE SESIÓN MALICIOSOS	CLASIFICACIÓN GLOBAL
India	2 867 867 749	4
China	2 805 330 412	5
Tailandia	2 626 767 167	7
Indonesia	2 328 720 242	8
Vietnam	2 166 055 670	9
Singapur	1 568 843 384	13
Malasia	1 547 306 924	15
Japón	845 793 217	18
Taiwán	817 736 419	19
Corea del Sur	737 126 412	20

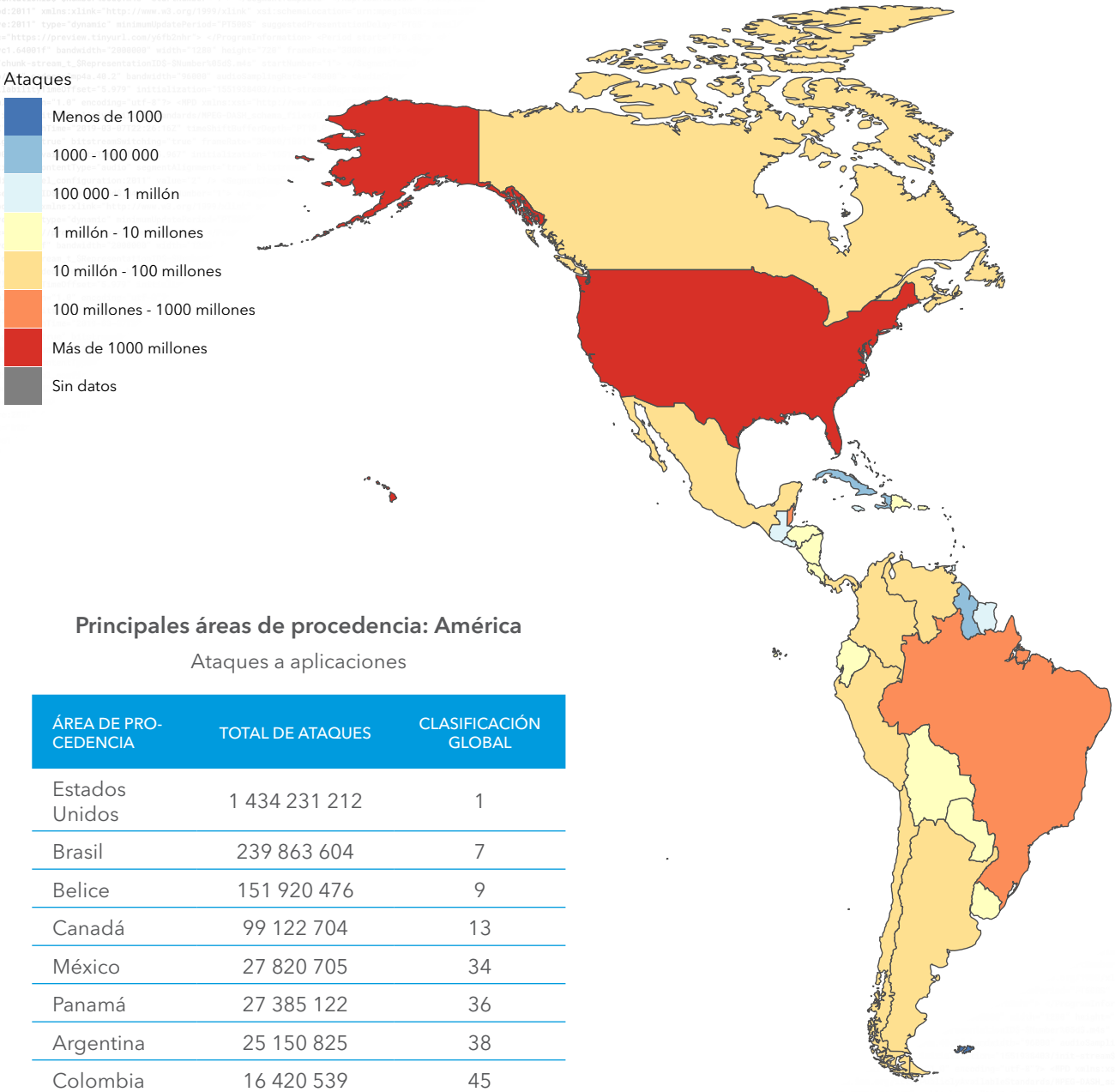
Ataques diarios a aplicaciones web

Noviembre de 2017 – septiembre de 2019



Fuentes de ataques a aplicaciones web: América

Noviembre de 2017 – septiembre de 2019



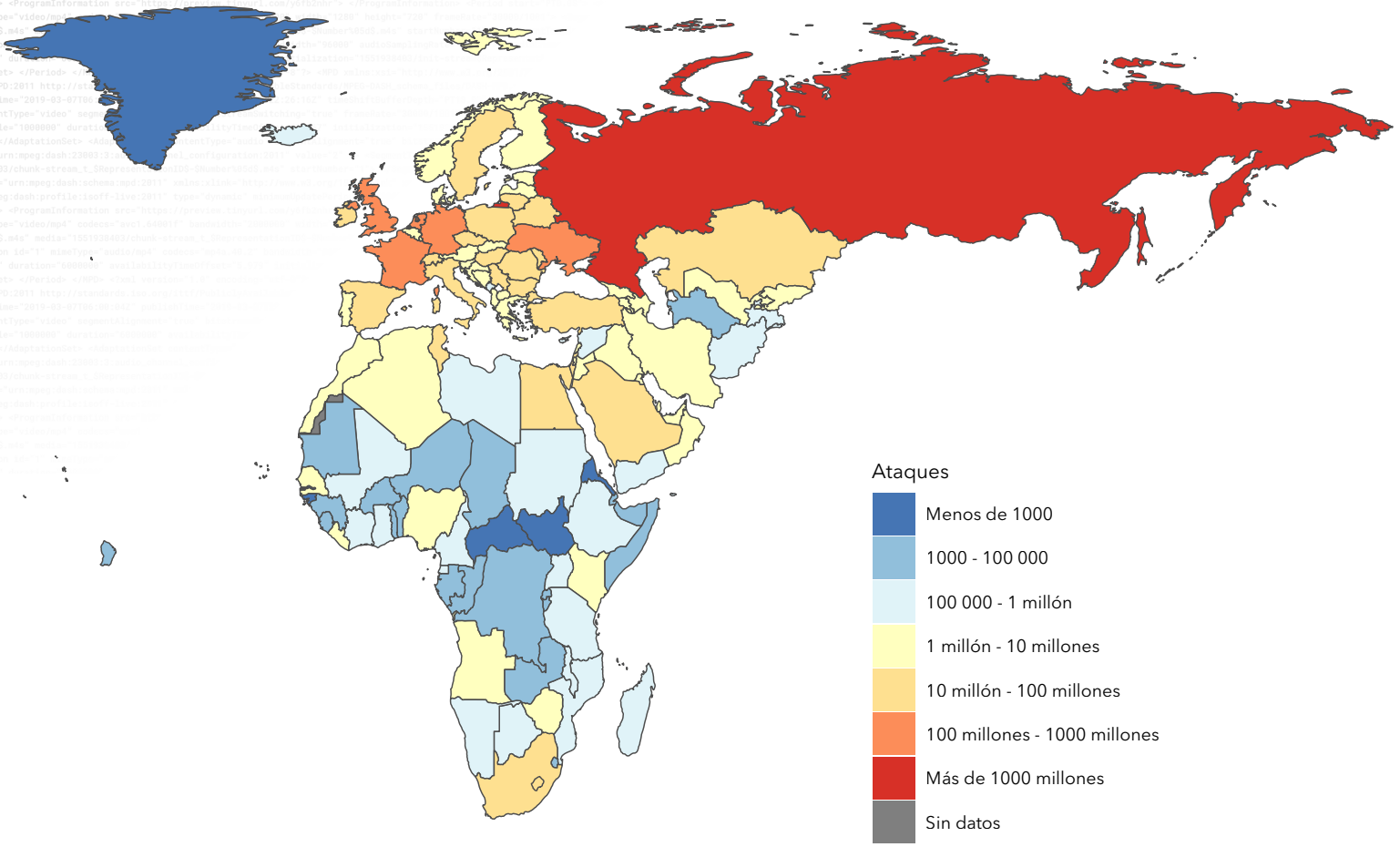
Principales áreas de procedencia: América

Ataques a aplicaciones

ÁREA DE PRO-CEDENCIA	TOTAL DE ATAQUES	CLASIFICACIÓN GLOBAL
Estados Unidos	1 434 231 212	1
Brasil	239 863 604	7
Belice	151 920 476	9
Canadá	99 122 704	13
México	27 820 705	34
Panamá	27 385 122	36
Argentina	25 150 825	38
Colombia	16 420 539	45
Venezuela	16 147 307	47
Chile	12 827 683	50

Fuentes de ataques a aplicaciones web: EMEA

Noviembre de 2017 – septiembre de 2019



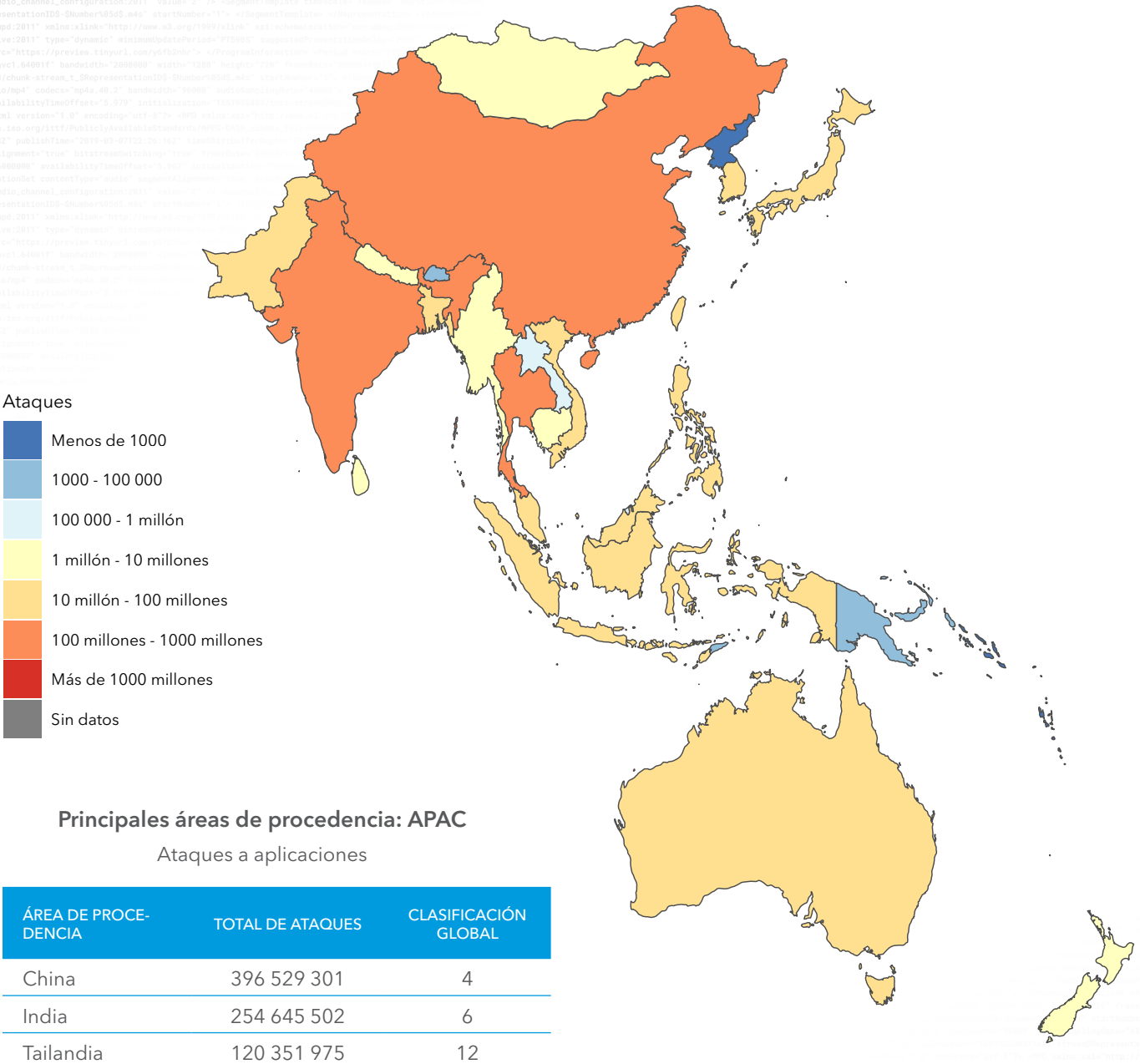
Principales áreas de procedencia: EMEA

Ataques a aplicaciones

ÁREA DE PROCEDENCIA	TOTAL DE ATAQUES	CLASIFICACIÓN GLOBAL
Rusia	1 093 219 355	2
Países Bajos	414 257 266	3
Ucrania	288 844 085	5
Alemania	200 129 170	8
Francia	148 147 042	10
Reino Unido	141 076 862	11
Irlanda	93 537 634	14
Turquía	88 376 455	16
Rumanía	69 929 767	20
Italia	52 615 647	24

Fuentes de ataques a aplicaciones web: APAC

Noviembre de 2017 – septiembre de 2019



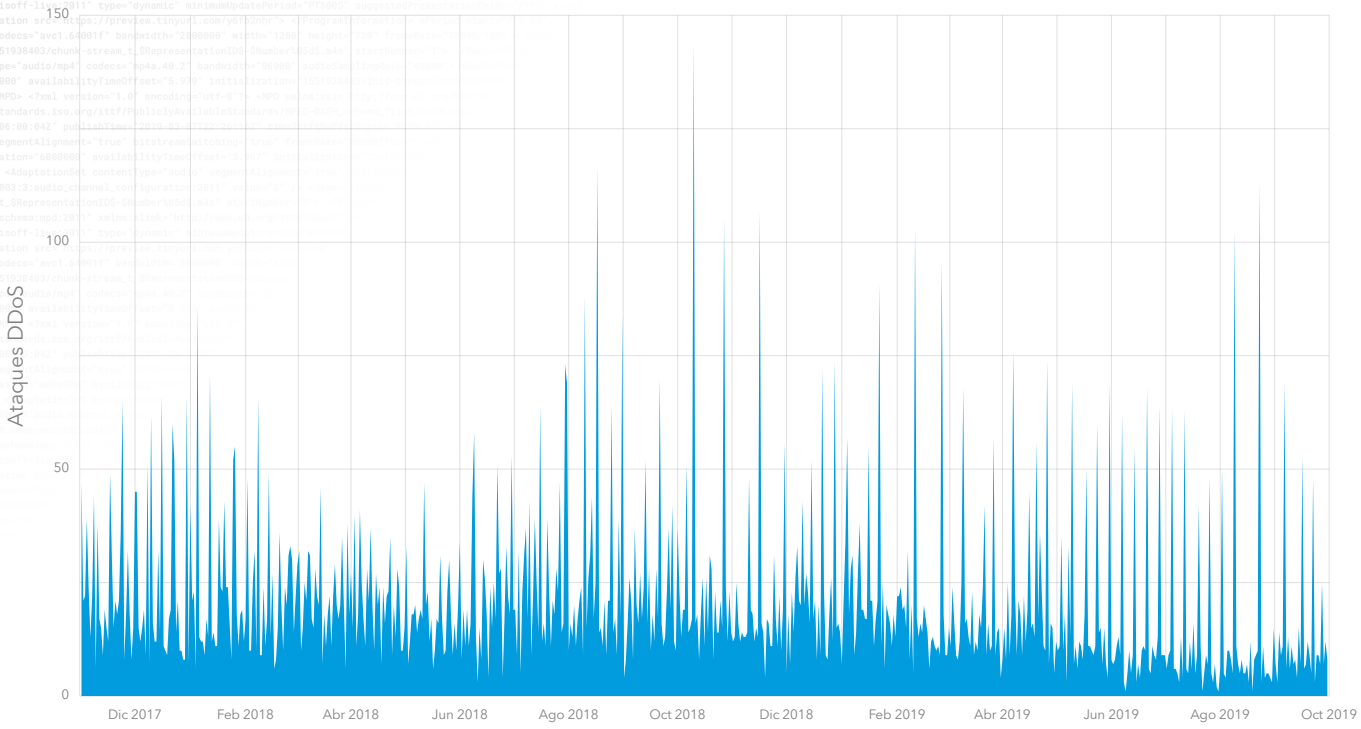
Principales áreas de procedencia: APAC

Ataques a aplicaciones

ÁREA DE PROCEDENCIA	TOTAL DE ATAQUES	CLASIFICACIÓN GLOBAL
China	396 529 301	4
India	254 645 502	6
Tailandia	120 351 975	12
Singapur	91 057 766	15
Indonesia	83 441 813	17
Japón	76 396 164	18
Vietnam	63 455 055	22
Taiwán	57 639 687	23
Hong Kong	49 977 066	25
Corea del Sur	43 552 997	27

Ataques DDoS diarios

Noviembre de 2017 – septiembre de 2019



Créditos

Colaboradores de Estado de Internet / Seguridad

VOLUMEN 5, NÚMERO 1

Ben Tang
Especialista en datos

Elad Shuster
Investigador de seguridad y responsable sénior

Chad Seaman
Equipo de respuesta a incidentes y de inteligencia en seguridad, sénior II

Larry Cashdollar
Equipo de respuesta a incidentes y de inteligencia en seguridad, sénior II

Moshe Zioni
Director de Investigación de amenazas

Gabriel Bellas
Responsable de Servicios globales

Autora invitada: Amanda Berlin
Mental Health Hackers

VOLUMEN 5, NÚMERO 2

Tony Lauro
Responsable sénior de Estrategia de seguridad

Moritz Steiner
Arquitecto principal

Kyle Schomp
Ingeniero de rendimiento sénior II

Rami Al-Dalky
Becario

VOLUMEN 5, EDICIÓN ESPECIAL SOBRE EL SECTOR MULTIMEDIA: CREDENTIAL STUFFING: ATAQUES Y MERCADOS

Shane Keats
Director de Marketing global del sector, contenido multimedia y entretenimiento

Steve Ragan
Investigador y redactor técnico sénior

Martin McKeay
Director editorial

VOLUMEN 5, NÚMERO 3

Elad Shuster
Investigador de seguridad y responsable sénior

Lydia LaSeur
Especialista en análisis de datos

Tim April
Arquitecto principal

Steve Ragan
Redactor técnico sénior

Martin McKeay
Director editorial

VOLUMEN 5, NÚMERO 4

Elad Shuster
Investigador de seguridad y responsable sénior

Or Katz
Investigador de seguridad y responsable principal

Tim April
Arquitecto principal

Colaboradores de Estado de Internet / Seguridad

VOLUMEN 5, NÚMERO 4 (CONT.)

Lydia LaSeur
Especialista en análisis de datos

Steve Ragan
Redactor técnico sénior

VOLUMEN 5, EDICIÓN ESPECIAL SOBRE EL SECTOR MULTIMEDIA: MEDIOS DE COMUNICACIÓN BAJO ATAQUE

Omri Hering
Analista de datos sénior

Lydia LaSeur
Especialista en análisis de datos

VOLUMEN 5, NÚMERO 5

Eric Kloster
Director de ingeniería

Lorenz Glaser
Ingeniero de seguridad sénior II

Or Katz
Investigador de seguridad y responsable principal

Lydia LaSeur
Especialista en análisis de datos

Paul O'Leary
Científico de datos principal,
Ingeniería de inteligencia ante amenazas

EQUIPO EDITORIAL DEL VOLUMEN 5, NÚMEROS 1 A 6

Martin McKeay
Director editorial

Amanda Fakhreddine,
Redactora técnica sénior y editora jefe

Steve Ragan
Redactor técnico sénior

Lydia LaSeur
Especialista en análisis de datos

EQUIPO DE MARKETING Y CREATIVOS PARA EL VOLUMEN 5, NÚMEROS 1 A 6

Benedikt Van Holt
Dirección de arte

Brendan John O'Hara
Diseño gráfico

Georgina Morales Hampe
Gestora del proyecto

Kylee McRae
Directora del programa

Murali Venukumar
Director del programa