SOTI

10 YEARS
OF SECURITY INSIGHT

Volumen 10, número 06

El sector sanitario bajo el microscopio

Ataques centrados en las aplicaciones y API

Akamai

Estado de Internet / Seguridad

Índice

2 *Columna de invitado de Untangle Health*: De la vulnerabilidad a la visibilidad: descifrando el panorama de la ciberseguridad en el sector sanitario

3 Introducción

5 Datos clave

6 Las aseguradoras corren un gran riesgo de ataques a sus API

9 El número de ataques DDoS contra organizaciones de ciencias de la vida está aumentando

13 Los proveedores de atención sanitaria se encuentran bajo asedio

16 Consideraciones sobre cumplimiento

18 Actuar: recomendaciones de mitigación

20 Metodología

21 Créditos

De la vulnerabilidad a la visibilidad: descifrando el panorama de la ciberseguridad en el sector sanitario

La situación del sector sanitario puede resumirse en una sola palabra: vulnerabilidad. Para solucionar este problema, el tema principal que abordar en este sector en 2024 debería ser la visibilidad. La gran cantidad de plataformas, software de terceros y procesos de intercambio de datos a gran escala hace necesaria una mayor visibilidad. Sin embargo, los avances técnicos se están produciendo a un ritmo tan rápido en las organizaciones sanitarias que son muchas las que tienen dificultades para ver el estado real de sus ecosistemas. Además de la complejidad, nos encontramos con medidas de cumplimiento que exigen compartir más información, pero con controles más estrictos. Aunque se trata del siguiente paso lógico para acabar con los fosos de datos y los monopolios de redes, incorpora factores de sofisticación técnica que, a menudo, hacen que sean insuficientes las medidas de seguridad con las que cuenta la mayor parte del sector, si dejamos a un lado, claro está, a los proveedores más importantes.

Los atacantes están viendo una cosa: la oportunidad. Conforme las distintas áreas de la atención sanitaria abren sus sistemas para intercambiar la información más confidencial de nuestra sociedad, estamos pasando a combinar nuevos sistemas y estándares con décadas de infraestructura heredada. Está claro que, si bien esa infraestructura heredada supone, en sí misma, una deuda técnica potencialmente enorme, también ofrece un entorno óptimo en el que los agentes maliciosos pueden lograr lo que pretenden.

Lamentablemente, no es sorprendente ver el aumento del número de ataques contra la ciberseguridad en el sector sanitario. En concreto, en Estados Unidos, muchas organizaciones sanitarias han venido considerando la seguridad cibernética como una tarea de cumplimiento de requisitos durante años en la presentación de propuestas y la evaluación de proveedores. En lugar de desarrollar competencias internas, las organizaciones se han dedicado simplemente a exigir a los proveedores que cuenten con la certificación SOC 2 de los marcos HITRUST o HIPAA, además de usar acuerdos de socios comerciales para que sean estos proveedores los que asuman el riesgo. Si bien es un buen comienzo, seguimos viendo cómo titular tras titular se anuncian importantes problemas financieros, interrupciones operativas o, lo que es peor, amenazas a la seguridad de los pacientes en el sector sanitario. Con esto vemos que se crea cierto revuelo, pero si tenemos en cuenta que entre una cuarta parte y la mitad de los 1000 principales hospitales y sistemas sanitarios utilizan el mismo sistema de comprobación de requisitos en hojas de cálculo para aprobar e incorporar proveedores, somos conscientes de que tenemos un problema.

Merece la pena abordar el hecho de que las aseguradoras están más expuestas que nunca, ya que las medidas de cumplimiento hacen que tengan que dejar atrás sus sistemas locales por lotes del pasado para cumplir los requisitos de datos basados en API del ecosistema moderno. Si bien en este nuevo panorama las aseguradoras pueden acceder a datos clínicos que han estado buscado durante años, el intercambio abierto es una nueva forma de hacer negocios que conlleva nuevos tipos de riesgos. Las aseguradoras, que almacenan información financiera y médica, deben proteger su infraestructura y planificar de forma minuciosa la mejora de su estrategia de ciberseguridad mientras cumplen cada nueva normativa.

Conclusión: estos cambios del mercado han llegado para quedarse. El sector sanitario ya no podrá abandonar los requisitos de API y de la nube. Aunque resulta comprensible la preocupación por lo que representan estos cambios para la seguridad, esta importancia del intercambio abierto de datos es fundamental para un sector que, históricamente, ha estado lleno de silos de datos.

Neil Jennings
Vicepresidente de Untangle Health

Chris Notaro
Director ejecutivo de Untangle Health

Introducción

El sector sanitario se enfrenta a algunos desafíos únicos en lo que respecta a la ciberseguridad.

- Lo que está en juego puede ser cuestión de vida o muerte.
- El valor que tiene esta información está entre los más altos de cualquier sector.
- La infraestructura incluye tanto sistemas heredados como dispositivos del Internet de las cosas médicas (IoMT).
- Los sistemas tienen un carácter federado y, en ocasiones, interdependiente.
- Los requisitos de cumplimiento figuran entre los más exigentes.

En este informe sobre el estado de Internet (SOTI), analizamos los datos de amenazas y las tendencias relacionadas con los riesgos en el ecosistema de la atención sanitaria. Las dos amenazas que están teniendo un mayor impacto en este sector son los ataques a aplicaciones web y API, así como los ataques distribuidos de denegación de servicio (DDoS).

Los participantes de todo el ecosistema sanitario (aseguradoras, proveedores y empresas farmacéuticas y de ciencias de la vida) también se enfrentan a desafíos específicos que deberían ser la base de su estrategia de seguridad.

Las aseguradoras cuentan con un acceso sólido a los datos clínicos y financieros para determinar la elegibilidad, la cobertura y los pagos, además de ser un nexo clave para compartir datos en todo el sector.

Las organizaciones del sector farmacéutico y de ciencias de la vida se han dado cuenta de que el punto de mira de los atacantes son sus innovaciones, entre ellas el uso de la inteligencia artificial y el aprendizaje automático (ML) para analizar grandes conjuntos de datos de innumerables aplicaciones, lo que los ha colocado claramente en la encrucijada entre la innovación y el riesgo.

Los fondos de los proveedores de atención sanitaria se canalizan principalmente hacia innovaciones clínicas como las videoconsultas y el floreciente IoMT, con un menor gasto organizativo en funciones más tradicionales, como los enfoques de la ciberseguridad en constante cambio, que son fundamentales para contar con resiliencia organizativa.

La tendencia hacia la interoperabilidad permite obtener mejores resultados financieros y para los pacientes, pero supone riesgos como, por ejemplo, los ataques a aplicaciones web y API.

Si adoptamos una perspectiva histórica, el ecosistema sanitario ha sido blanco de los atacantes durante años. En 2024, por decimotercer año consecutivo, el sector sanitario ha tenido los costes por filtraciones de datos más altos de todos los sectores, con un coste medio de 9,77 millones de dólares, lo que supone un aumento muy importante con respecto al de los servicios financieros, el siguiente sector más cercano, con 6,08 millones de dólares.

Las API son una de las principales tecnologías que afectan a todos los subsectores del sector sanitario. Permiten compartir datos entre proveedores, aseguradoras, pacientes y otras terceras partes, como los sistemas de expedientes médicos electrónicos, las empresas de dispositivos médicos y las redes de intercambio de información sanitaria. La tendencia hacia la interoperabilidad permite obtener mejores resultados financieros y para los pacientes, pero supone riesgos como, por ejemplo, los ataques a aplicaciones web y API.

Otra amenaza habitual para la capa de aplicación son los ataques DDoS. Son el arma preferida actualmente en Europa, Oriente Medio y África (EMEA), lo que probablemente se pueda atribuir a los acontecimientos geopolíticos y a los grupos hacktivistas prorrusos de la región. Sin embargo, ningún país o región es inmune a los ataques, ya que el número de grupos que realizan ataques DDoS, así como las tácticas, las técnicas y los procedimientos que utilizan, están sometidos a constantes cambios.

Datos clave

41 %

Porcentaje de ataques a API en el ecosistema sanitario dirigidos a compañías aseguradoras

Los ataques a las API crecen de forma constante en el ecosistema sanitario, especialmente los ataques a compañías aseguradoras debido a la gran cantidad de información que poseen: información sanitaria protegida (PHI), datos de reclamaciones e información financiera.

La proliferación de las API plantea riesgos importantes, como el acceso no autorizado a los datos

La proliferación de las API, o el incremento no regulado de API dentro de las organizaciones, puede generar importantes brechas de seguridad debido a que pasan desapercibidas y a que surgen fuera de los controles de seguridad. Como consecuencia, la proliferación de API amplía la superficie de ataque de una organización y plantea riesgos como el acceso no autorizado a datos confidenciales.

88 %

Porcentaje de ataques DDoS a la capa 7 contra organizaciones farmacéuticas de la región EMEA

Las empresas farmacéuticas de la región EMEA experimentaron el mayor volumen de ataques DDoS a la capa 7, seguidas de las de la región de Norteamérica y Asia-Pacífico y Japón (APJ). Un análisis más detallado de los datos de la primera mitad de 2024 revela que el número de ataques contra EMEA y Norteamérica va camino de superar el total de cada una de las regiones en 2023.

21 MILLONES

Media mensual de ataques a las API y aplicaciones web contra proveedores de atención sanitaria

La necesidad de contar con datos interoperables y otros requisitos de cumplimiento han impulsado el crecimiento del uso de API y aplicaciones web, lo que, a su vez, ha generado riesgos de seguridad tanto para los proveedores como para los pacientes.

415 MILLONES

Media mensual de ataques DDoS a la capa 7 contra proveedores de atención sanitaria

El sector sanitario está experimentando un aumento de los ataques DDoS, impulsados por el hacktivismo y la situación geopolítica actual. Estos ataques pueden provocar interrupciones y perturbaciones que pongan en peligro la evolución del paciente. En 2023, Killnet lanzó una campaña DDoS a gran escala que afectó principalmente a las organizaciones de proveedores.

Las aseguradoras corren un gran riesgo de ataques a sus API

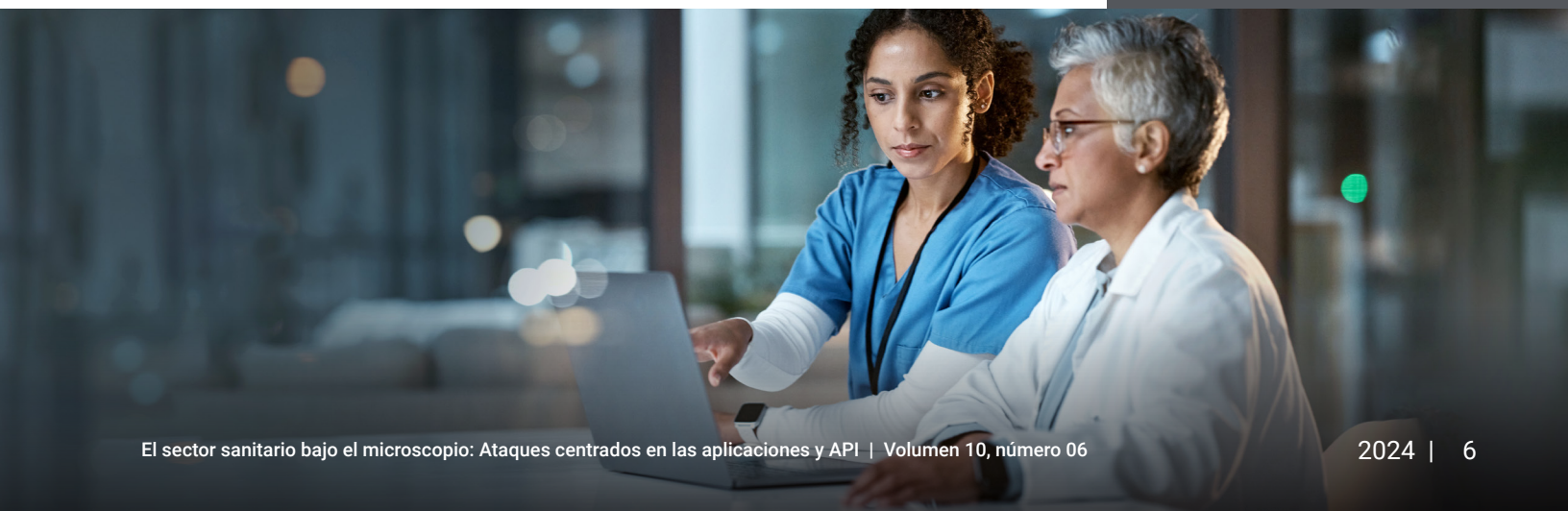
Aunque el uso extendido de API por parte de las aseguradoras para recopilar y procesar datos en todo el ecosistema sanitario tiene enormes ventajas, también tiene otras implicaciones, como tener que cumplir muchos requisitos y los posibles riesgos para la seguridad. Los ciberdelincuentes y los agregadores atacan estos recursos y hacen un uso indebido de ellos, lo que puede provocar problemas de seguridad y privacidad.

Para las aseguradoras, los ataques basados en las API también pueden causar interrupciones del servicio que afectan a operaciones de inscripción abierta y reclamaciones, provocar tiempos de inactividad con un alto coste y dañar la marca de la empresa. El ataque sistémico que obstaculizó gravemente el procesamiento de pagos en las farmacias de Estados Unidos en febrero de 2024 es un ejemplo reciente y doloroso.

Tendencias de ataques a API

La investigación de Akamai reveló que, desde enero de 2023 hasta junio de 2024, el 41 % de los ataques a las API dirigidos al ecosistema sanitario tenían como objetivo a las aseguradoras, lo que indica que estas se enfrentan a un mayor riesgo de uso indebido de las API por ataques, hecho que tiene que ver con la importancia que tiene para las aseguradoras que el sistema sanitario siga funcionando, ya que aproximadamente el 67 % del gasto total sanitario de EE. UU. lo realizaron las aseguradoras en 2022.

Observamos una tendencia similar en otros sectores regulados, especialmente en aquellos que operan con sistemas de pago. El sector financiero, por ejemplo, ha experimentado un gran avance en su proceso de transformación digital y ya está utilizando API más integradas como parte de sus modelos de negocio. La banca abierta está impulsando el uso de las API y, de ese modo, genera más riesgos de seguridad. Por ello, el sector financiero está sufriendo un mayor número de ataques centrados en las API, como se comenta en nuestro informe sobre el estado de Internet en materia de seguridad (SOTI) de las API.



Al examinar más detenidamente los datos de los ataques a las API de las aseguradoras, los investigadores de Akamai han observado fluctuaciones en la actividad durante el periodo de 18 meses comprendido entre enero de 2023 y junio de 2024, especialmente por trimestres. La tendencia general al alza de cada trimestre puede reflejar la sincronización entre sistemas al final del trimestre que se produce para conciliar los datos previstos y los reales. Sin embargo, el aumento general del cuarto trimestre de 2023 puede atribuirse a atacantes cuyos objetivos eran los periodos de inscripción abierta para interrumpir las operaciones (Figura 1).

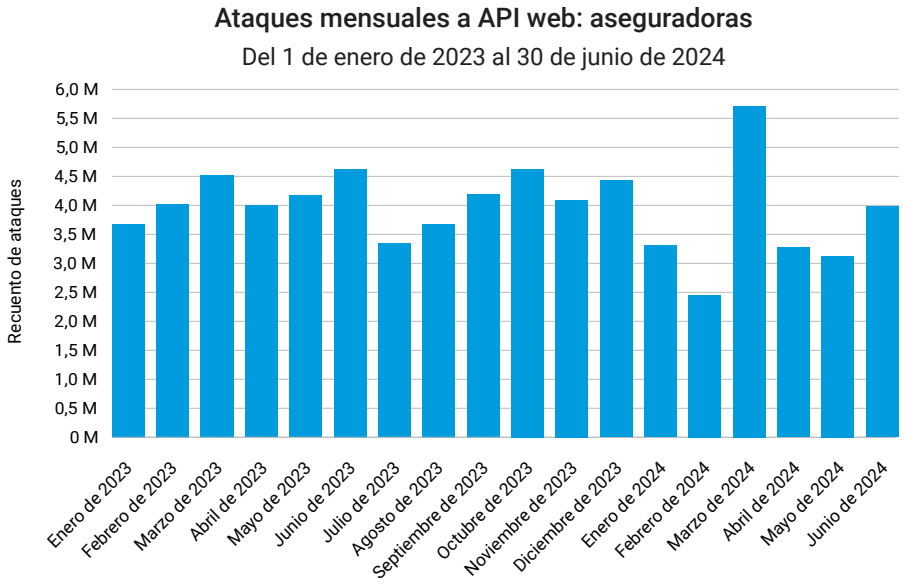


Fig. 1: Los ataques web a las API experimentaron una tendencia al alza en todos los trimestres, con un aumento global en el cuarto trimestre de 2023

Uso indebido de las API y problemas de seguridad críticos en todos los sectores

Aunque muchos de los problemas de seguridad de las API son específicos del sector sanitario, los aspectos básicos de las API son similares en todos los sectores, por lo que merece la pena revisar algunos de los riesgos más técnicos que todos debemos mitigar. En primer lugar, debemos concentrarnos en los riesgos destacados por los 10 principales riesgos de seguridad de API según OWASP. Pero también debemos asegurarnos de que nuestros desarrolladores y personal de TI conozcan las vulnerabilidades más comunes que hemos clasificado como problemas de estrategia y de tiempo de ejecución.

- Con **problemas de estrategia** hacemos referencia a los fallos en la implementación de API de la empresa. Las alertas que indican problemas de estrategia ayudan a los equipos de seguridad a identificar y corregir vulnerabilidades de alta prioridad antes de que los atacantes las puedan explotar. Entre los problemas de estrategia habituales se encuentran los terminales en la sombra y los datos confidenciales en una URL.

- Los **problemas de tiempo de ejecución** son amenazas activas o comportamientos que requieren una respuesta urgente. Estas alertas críticas son más sutiles que otros tipos de alertas de seguridad, ya que adoptan la forma de abuso de API (frente a otros intentos de vulneración de la infraestructura más explícitos). Entre los problemas de tiempo de ejecución habituales se incluyen los intentos de acceso a recursos no autenticados y el scraping de datos.

También es fundamental tomar distancia y analizar los tres principales desafíos generales a los que se enfrentan las API para garantizar que su programa de seguridad cubra el abuso y explotación de las API.

1. **Visibilidad**: ¿Cuenta con controles técnicos y de procesos para garantizar que su programa proteja todas las API? Este es un problema clave, ya que las API suelen formar parte de la transformación o estar integradas en los nuevos productos, por lo que muchas de ellas no tienen el mismo nivel de indicaciones, protecciones y validaciones que una presencia web tradicional.

2. **Vulnerabilidades:** ¿Sus API siguen las prácticas recomendadas para el desarrollo? ¿Evita los problemas de codificación deficiente más comunes según OWASP? Por último, ¿realiza un seguimiento y comprobaciones de vulnerabilidades?

3. **Abuso de la lógica empresarial:** ¿Cuenta con un estándar de tráfico esperado? ¿Ha establecido qué se considerarían actividades sospechosas?

Las respuestas a estas preguntas son la base de lo que su equipo debe comprender. Los objetivos generales deberían ser tener visibilidad y la capacidad para llevar a cabo investigaciones, así como tener procesos establecidos para mitigar rápidamente las amenazas. Esto se aplica tanto a las API internas como a las que tienen acceso los pacientes.

Un mejor rendimiento puede traducirse en un mayor riesgo

El rendimiento se está convirtiendo en una preocupación cada vez mayor, ya que los pacientes exigen el mismo nivel de experiencia de usuario en todas sus aplicaciones. Esto implica que el ecosistema sanitario deba estar protegido contra ataques de denegación de servicio, así como contra ataques de uso indebido. Además, los proveedores deben cumplir requisitos normativos de transparencia, lo que hace que sea necesario disponer de la información en el momento oportuno.

La proliferación de las API puede causar una visibilidad deficiente que se vuelve aún más turbia a medida que se amplía la superficie de ataque. Las API suelen formar parte de proyectos de transformación digital complejos, por lo que puede que no estén en el radar de las organizaciones sanitarias y, mucho menos, los programas de seguridad.

Los tipos de datos, tanto médicos como financieros, implicados en las actividades empresariales diarias están muy regulados y pueden ser objeto de ataque por parte de los ciberdelincuentes, lo que viene a unirse a los desafíos a los que se enfrentan las aseguradoras.

Las API suelen formar parte de proyectos de transformación digital complejos, por lo que puede que no estén en el radar de las organizaciones sanitarias y, mucho menos, los programas de seguridad.

El número de ataques DDoS contra organizaciones de ciencias de la vida está aumentando

La relevancia de la ciberseguridad farmacéutica se acentuó durante la pandemia de COVID-19, cuando los atacantes consideraron un blanco la investigación para el desarrollo de vacunas, los datos de ensayos, la fabricación, la producción y la implementación. Actualmente, el sector sanitario se considera una infraestructura crítica de EE. UU. y la nueva financiación bipartidista exige mayores requisitos de resiliencia en todos los sectores considerados críticos. Las razones son obvias:

- Las tensiones internacionales continúan aumentando en todo el mundo, y la situación geopolítica es un factor muy tenido en cuenta por los ejecutivos que respondieron a la 25ª Encuesta Global Anual de CEO de PwC. Para casi un tercio de los encuestados el conflicto geopolítico amenaza el crecimiento de sus empresas, mientras que para más de dos tercios es un factor que prevén que provoque interrupciones en la cadena de suministro.
- Estrategias como el abastecimiento localizado y el mayor uso de la tecnología de blockchain pueden permitir a las empresas farmacéuticas aumentar la resiliencia y mejorar el impacto clínico y en el negocio.
- De los datos mundiales de Akamai para el sector de las ciencias de la vida podemos deducir que los ataques DDoS (y el número de grupos que los perpetran) no dejan de crecer; la resiliencia es justo lo que este sector necesita.

EMEA, objetivo de los ataques DDoS a la capa de aplicación contra empresas farmacéuticas

La investigación de Akamai reveló que, entre enero de 2023 y junio de 2024, la región de EMEA sufrió el 88 % del total de ataques DDoS a la capa de aplicación (capa 7) dirigidos contra empresas farmacéuticas, mientras que las regiones de Norteamérica y APJ representaron el 7 % y el 5 % de esos ataques, respectivamente. Si se analizan los datos de la primera mitad de 2024, podemos ver que la concentración de ataques tanto en EMEA como en Norteamérica iba en aumento y en camino de eclipsar el número total de ataques de cada región en 2023 (Figura 2).

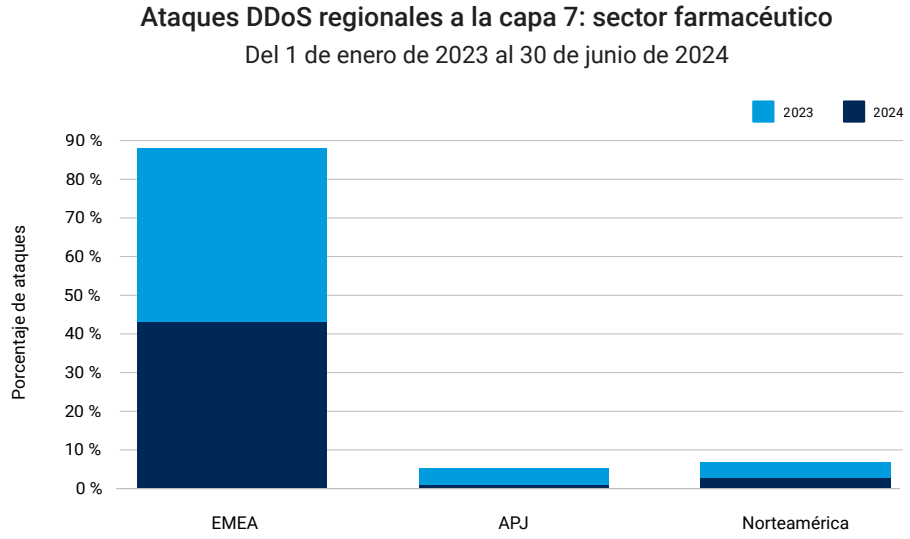


Fig. 2: La concentración de ataques DDoS a la capa 7 en EMEA continúa de 2023 a 2024 y aumentó en la primera mitad de 2024, mientras que los ataques en Norteamérica también aumentaron

A diferencia de los ataques DDoS a las capas 3 y 4, cuyo objetivo es saturar la infraestructura de red y de la capa de transporte, los ataques DDoS a la capa 7 tienen en el punto de mira funcionalidades específicas de las aplicaciones o el propio servidor de aplicaciones. Pueden causar daños importantes incluso con una cantidad relativamente pequeña de tráfico malicioso.

Los ataques DDoS a la capa 7 tienen como objetivo los recursos de nivel de aplicación, como la CPU y la memoria, por lo que la aplicación o el servicio objeto del ataque pueden ralentizarse o dejar de responder por completo, incluso aunque la red siga estando disponible.

Aumento de los ataques DDoS al sector sanitario y de las ciencias de la vida en la Unión Europea

En el informe ENISA 2023 Threat Landscape: Health Sector, se confirma un mayor número de ataques DDoS en el sector sanitario y de las ciencias de la vida en la Unión Europea. Resulta interesante observar que los países "más conflictivos" desde el punto de vista de los incidentes cibernéticos (especialmente Francia, Alemania y Países Bajos) que aparecen en el informe corresponden a aquellos con una mayor concentración geográfica de empresas farmacéuticas y biotecnológicas que figuran en la lista de las 1000 mayores empresas de la Unión Europea en 2022.

ENISA (Agencia de la Unión Europea para la Ciberseguridad) atribuye el aumento de los ataques DDoS a los acontecimientos geopolíticos y a grupos hacktivistas prorrusos como Killnet.

Las empresas de ciencias de la vida de los EE. UU. son el siguiente objetivo

Killnet atacó a hospitales europeos antes de pasar a tener en el punto de mira a los hospitales de prácticamente todos los estados de EE. UU. Aunque esos ciberataques a los hospitales fueron los que más atención acapararon en los titulares, un informe de abril de 2023 del Departamento de Salud y Servicios Humanos (HHS) de EE. UU. señala que, en realidad, fueron las empresas farmacéuticas y biotecnológicas las que tuvieron el porcentaje de ataques DDoS más alto por parte de Killnet.

Dado que los Estados Unidos tienen una cuota de mercado mundial de ciencias de la vida mayor (50 %) que la región de EMEA (34 %), es razonable esperar que se intensifique la amenaza de ataques DDoS contra empresas farmacéuticas con sede en Estados Unidos.

Pero ningún país o zona geográfica queda inmune. India, uno de los mayores productores y exportadores de medicamentos genéricos de todo el mundo, sufrió graves consecuencias el año pasado después de un incidente de seguridad, gracias al que se filtraron 17 TB de datos confidenciales de la empresa. La banda de ransomware y el atacante ALPHV/BlackCat asumieron la responsabilidad de otro ataque de ransomware que incluía información confidencial sobre proveedores, clientes y documentos de 1500 empleados estadounidenses.

¿Cuáles son las tácticas que utilizan los distintos atacantes?

En el informe de ENISA se menciona a ALPHV/Black Cat como uno de los principales grupos de atacantes del sector de las ciencias de la vida en la región EMEA, el mismo grupo que golpeó la cadena de suministro de EE. UU. a principios de este año.

Al igual que Killnet, también se menciona en el informe a Anonymous Sudan como organización criminal con motivaciones políticas, que se centró en un primer momento en grupos de proveedores, pero que ahora está expandiendo sus objetivos para incluir a otros actores del ecosistema sanitario.

Esa expansión hace que acontecimientos recientes como la reivindicación de responsabilidad de Anonymous Sudan por los recientes ataques DDoS contra OpenAI sean aún más preocupantes. El grupo afirma que utilizó la botnet Skynet, que recientemente incorporó la capacidad de lanzar ataques DDoS de capa 7, para saturar las aplicaciones y generar errores.

Los riesgos implicados exigen un enfoque conservador

Las empresas farmacéuticas llevan mucho tiempo siendo líderes del sector sanitario en el uso de la inteligencia artificial (IA), en concreto el aprendizaje automático (ML), y se han beneficiado de la capacidad de la IA para analizar grandes conjuntos de datos de infinidad de aplicaciones. Entre las ventajas se incluyen el poder detectar antes la enfermedad, descubrir fármacos más rápido y mejorar el proceso de fabricación de estos. Sin embargo, al igual que ocurre en otros sectores que están llevando a cabo una transformación digital (como el de los servicios financieros), las ciencias de la vida se encuentran en la encrucijada entre innovación y riesgo.

Fueron las empresas farmacéuticas y biotecnológicas las que tuvieron el porcentaje de ataques DDoS más alto por parte de Killnet.

Las organizaciones farmacéuticas están tomando partido. Al analizar cómo otros sectores regulados gestionan los ataques DDoS a la capa 7, los investigadores de Akamai descubrieron que, en lo que respecta al porcentaje de acciones de "denegación" frente a "alerta" aplicadas, las empresas farmacéuticas adoptan políticas conservadoras que deniegan en más ocasiones la actividad anómala (Figura 3).

Acción aplicada ante ataques DDoS a la capa 7 por subsector

Del 1 de enero de 2023 al 30 de junio de 2024

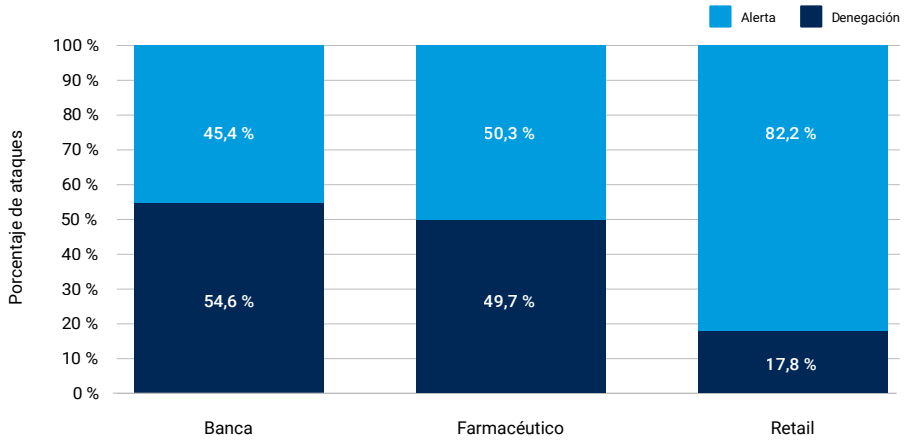


Fig. 3: En las empresas farmacéuticas y de ciencias de la vida se observa un alto porcentaje de acciones de denegación frente a alerta

Desde que informamos por primera vez de esta cifra de denegación frente a alerta en el periodo comprendido entre enero de 2023 y marzo de 2024, el nivel ha aumentado más de cuatro puntos porcentuales, donde las acciones de denegación han pasado del 45,5 % al 49,7 %, un importante incremento en un breve periodo.

Otros sectores, como los servicios financieros y la banca, también adoptan estas políticas conservadoras; tanto la banca como las ciencias de la vida se consideran infraestructuras críticas y, por lo tanto, están sometidas a muchas regulaciones, lo que explica muchas de las similitudes.

Además, en el caso de las organizaciones farmacéuticas, las consecuencias de un ataque DDoS que consiga sus objetivos pueden ser graves, y podrían poner en peligro la vida de las personas, al retrasar el acceso a medicamentos esenciales. Tiene toda la lógica tender a aplicar una acción de denegación y, a posteriori, investigar la actividad.

Por su parte, el sector del retail adopta una postura menos agresiva, lo que permite disponer de más tiempo para recibir una alerta y evaluar la actividad anómala antes de tomar medidas. Sin embargo, es posible que seamos testigos de un cambio hacia una tendencia hacia acciones de denegación entre los retailers si aparecen nuevas normativas, especialmente en relación con el uso de la IA o el ML.

Los investigadores de Akamai observaron que, cuando se habla del porcentaje de acciones de "denegación" frente a "alerta" aplicadas, las empresas farmacéuticas adoptan políticas conservadoras que deniegan la actividad anómala a un ritmo alto en comparación.

Los proveedores de atención sanitaria se encuentran bajo asedio

Citando el análisis de las filtraciones de datos del Departamento de Salud y Servicios Humanos (HHS) publicado en diciembre de 2023, el director de Seguridad del Centro de Análisis e Intercambio de Información Sanitaria declaró que se habían producido y notificado al HHS una media de 3604 filtraciones de registros de pacientes cada hora.

El número de ciberataques a proveedores y hospitales sigue en aumento. La conectividad e interoperabilidad impulsadas por las aplicaciones web y el uso obligado de las API ponen en riesgo a los proveedores y a los pacientes. Las vulnerabilidades no corregidas y la deuda técnica de la tecnología heredada constituyen un desafío de alto coste que utilizan los grupos de ransomware a su favor.

Y tanto la amenaza continua que suponen los ataques DDoS a hospitales atribuidos a grupos hacktivistas como el clima geopolítico están deteriorando la atención al paciente. Todo esto está derivando en filtraciones de datos de información sanitaria protegida (PHI), impactos negativos en la atención al cliente y, en algunos casos, problemas relacionados con la seguridad del paciente.

Los ataques se ceban con las organizaciones proveedoras

La investigación de Akamai reveló que durante el periodo de 18 meses que abarca el informe, desde enero de 2023 hasta junio de 2024, los ataques a las API y las aplicaciones web dirigidos a organizaciones de proveedores continuaron a un ritmo constante (Figura 4). Es probable que esta tendencia siga creciendo, con fluctuaciones, a medida que los ciberdelincuentes aprovechen las vulnerabilidades nuevas y de probada eficacia inherentes a los modelos de atención sanitaria, los métodos de distribución y los sistemas innovadores en constante evolución para atacar y hacer un uso indebido de las API y las aplicaciones web.

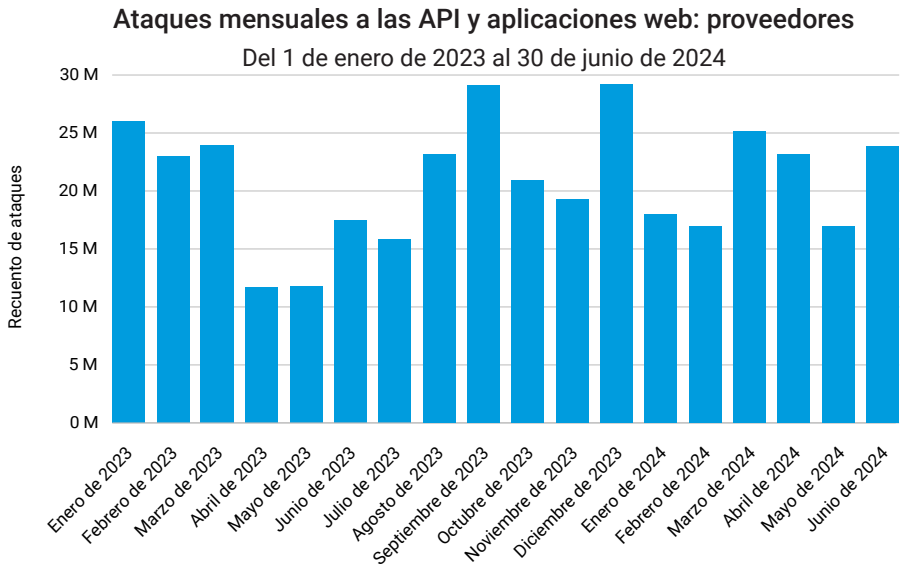
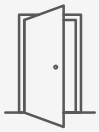


Fig. 4: Los ataques mensuales a las API y las aplicaciones web dirigidos a organizaciones de proveedores alcanzaron una media de 21 millones a nivel mundial (NOTA: Un cliente distorsionó los datos, por lo que fue excluido a efectos de la presentación del informe).



Las vulnerabilidades no corregidas y la deuda técnica de la tecnología heredada constituyen un desafío de alto coste que utilizan los grupos de ransomware a su favor.

La coordinación de la asistencia sanitaria mediante el uso compartido de datos y la interoperabilidad a través de aplicaciones web y las API se traduce en mejores resultados clínicos y financieros. Sin embargo, esto pone al sector de la atención sanitaria en una situación de riesgo importante, ya que las implicaciones de seguridad de las API aún no se conocen por completo.

Cómo equilibrar la coordinación de la asistencia sanitaria con el riesgo que suponen las vulnerabilidades

Teniendo en cuenta al gran número de registros de pacientes y los puntos de conectividad del sistema, es necesario que los proveedores de atención sanitaria optimicen la coordinación de la atención sanitaria al mismo tiempo que implementan controles para proporcionar visibilidad y mitigar de forma proactiva el riesgo que presentan las vulnerabilidades. Lograr este equilibrio suele presentar desafíos a la hora de implementar nuevas tecnologías e infraestructuras, como las API.

Los investigadores de Akamai estudiaron asimismo los ataques DDoS a la capa 7 dirigidos a organizaciones de proveedores durante el mismo periodo de 18 meses y detectaron una cadencia constante de interrupciones después de enero de 2023 (Figura 5). Podemos atribuirlo, en parte, a una campaña global de DDoS del grupo hacktivista prorruso Killnet contra el sector sanitario, enfocada especialmente en las organizaciones de proveedores de los Estados Unidos. Durante el periodo, los ciberdelincuentes siguieron aprovechando los ataques DDoS contra funcionalidades de las aplicaciones o contra las propias aplicaciones, lo que supuso un riesgo para la atención al paciente.

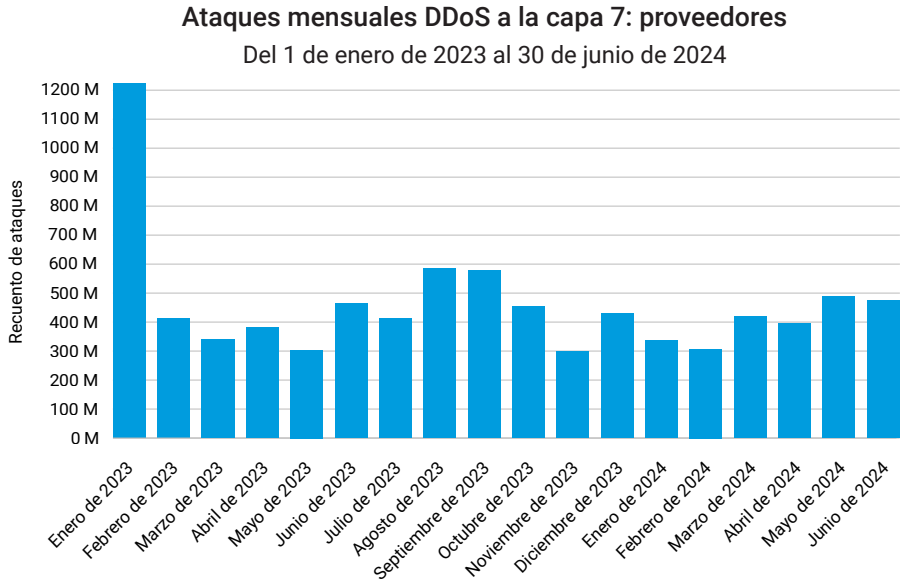


Fig. 5: Con la excepción de un aumento aislado en enero, los ataques mensuales DDoS a la capa 7 dirigidos a organizaciones de proveedores alcanzaron una media de 415 millones a nivel mundial

Los ataques DDoS en el sector sanitario están alcanzando nuevos récords de escala y velocidad

Por otro lado, un aumento de la actividad de DDoS, atribuido a acontecimientos geopolíticos y grupos hacktivistas, ha causado interrupciones que pueden poner en peligro la evolución de los pacientes. Todo el ecosistema sanitario se ha visto afectado: las organizaciones de proveedores fueron los objetivos más frecuentes en los ataques DDoS a gran escala de Killnet en 2023. El HC3 ha advertido que las interrupciones del servicio, incluso de unas pocas horas, pueden afectar a todo el abanico de operaciones diarias, desde las rutinarias hasta las críticas, con consecuencias potencialmente significativas.

Teniendo en cuenta que se producen más interacciones de atención sanitaria a través de aplicaciones, cada vez cobra más importancia para la experiencia del paciente poder recibir información y asistencia a tiempo. Por lo tanto, es fundamental asegurarse de que cuenta con la protección y los procesos necesarios.

Los ataques en varios frentes impiden la coordinación de la asistencia sanitaria

Además de los ataques DDoS, los proveedores se enfrentan a otros tipos de ataques populares. Los ataques de ransomware que limitan el acceso a los historiales clínicos y obligan a las ambulancias a desviarse evidencian que, sin acceso al historial médico, no es posible la coordinación entre los proveedores de atención sanitaria. Volver a los registros en papel supone un deterioro del seguimiento de las operaciones de atención al paciente, la comunicación entre departamentos clave y todos los servicios de pedidos.

Las organizaciones de proveedores fueron los objetivos más frecuentes en los ataques DDoS a gran escala Killnet de 2023.

Cuando los datos confidenciales se ven afectados, las organizaciones de proveedores también tienen que hacer frente al impacto de una filtración de datos. La explotación de vulnerabilidades en herramientas de software populares permite que atacantes no autorizados obtengan acceso a una valiosa fuente de datos, desde la PHI hasta la información médica y relativa a seguros médicos.

La protección del paciente debe incluir la protección de datos

Una parte de la atención al paciente es la capacidad de proteger y controlar el acceso a sus datos. Tradicionalmente, los presupuestos y los equipos de ciberseguridad del sector sanitario han sido escasos, lo cual ha contribuido a los desafíos que ahora se presentan en relación con la protección de los datos. Sin embargo, mientras los ciberataques contra los grupos de proveedores de atención sanitaria siguen generando titulares, los grupos de proveedores continúan potenciando asociaciones de protección externalizadas y aumentando la cobertura de los seguros cibernéticos.

La tendencia a mejorar la protección seguirá aumentando, a medida que los proveedores de atención sanitaria se beneficien de las actualizaciones de las políticas gubernamentales de EE. UU., que tienen como objetivo mejorar la resiliencia en los sectores de infraestructuras críticas.

Consideraciones sobre cumplimiento

El panorama normativo requiere cada vez más transparencia, lo que está impulsando el uso de API. Las medidas de cumplimiento están imponiendo muchos requisitos de intercambio de datos tanto a los proveedores como a las aseguradoras. Este intercambio tiene como objetivo permitir la interrelación de datos clínicos y financieros, que históricamente ha sido difícil para las partes, pero que es necesaria para la ejecución eficaz de la asistencia sanitaria basada en el valor (VBC).

El cambio hacia la VBC, es decir, la prestación de atención sanitaria teniendo en cuenta los costes, es un ejemplo excelente de la cantidad y variedad de información que ahora se debe compartir. Las aseguradoras han tenido acceso durante mucho tiempo a datos financieros de pacientes y proveedores. Sin embargo, el mayor número de puntos de datos de la VBC, así como el cumplimiento de la medicación y los ingresos hospitalarios, requieren un proceso continuo que no solo sea más innovador, sino que también permita un mayor nivel de interoperabilidad, y este precisa un medio para compartir estos datos. Las API son el vehículo.

La reciente regla final de interoperabilidad de CMS y acceso de pacientes exige que las aseguradoras mantengan tres categorías principales de API para permitir el intercambio constante de información entre pagadores, proveedores y pacientes:

1. API de acceso del paciente: potenciará el acceso de los miembros a sus propios datos médicos y, probablemente, aumentará la satisfacción de los miembros.

2. API de directorio de proveedores: permite a los miembros buscar proveedores de atención sanitaria e instalaciones en función de su ubicación y especialidad médica, lo cual mejora el acceso a la atención sanitaria.

3. API aseguradora-proveedor y API aseguradora-aseguradora: pueden ayudar a solucionar y minimizar las deficiencias en la atención al paciente y, posiblemente, reducir los servicios duplicados y costosos

Y, próximamente, la regla final de interoperabilidad y autorización previa de CMS exigiría a las aseguradoras afectadas adoptar una API adicional de autorización previa.

Las medidas de cumplimiento también están dictando el formato de las API a través del estándar Fast Healthcare Interoperability Resources (FHIR). Estos requisitos y estándares simplificarán y agilizarán la interoperabilidad entre los distintos sistemas, al tiempo que impulsan la seguridad. La expectativa de FHIR es que exista un programa de seguridad que incluya características básicas como un firewall de aplicaciones web, autenticación, cifrado, privacidad y microsegmentación.

Aunque los proveedores están obligados a compartir más datos que nunca, y en un formato estándar que les permita conectarse a las aplicaciones de salud del paciente (las que estos últimos elijan) en el momento necesario, la intención del estándar FHIR es reducir la carga administrativa y aumentar la transparencia. Por lo tanto, esto se traducirá en un mejor nivel de servicio para los pacientes.

Además, los retrasos al intercambiar datos pueden tener graves repercusiones de carácter médico (a menudo costosas), e incluso el tener que hacer frente a sanciones por bloqueo de la información. Por lo tanto, los proveedores que han migrado recientemente a la nube se están apresurando a implementar API externas con el nuevo formato para ajustarse a estas nuevas medidas de cumplimiento.

Aparte del riesgo que suponen los ataques centrados en API, los ataques relacionados con la disponibilidad, como DDoS y ransomware, siguen teniendo un efecto importante en todos los sectores, y el sector sanitario puede verse gravemente afectado. Las normativas que pretenden abordar estos tipos de ataques tienden a centrarse en la resiliencia. Por ejemplo, en Estados Unidos, el Departamento de Salud y Servicios Humanos (HHS) ha publicado una guía sobre DDoS para el sector sanitario (Healthcare Sector DDoS Guide). Además, la organización sin ánimo de lucro Healthcare Information Sharing and Analysis Center ha publicado un white paper sobre la resiliencia en el sector sanitario titulado Resilience is in our DNA (La resiliencia está en nuestro ADN).

Actuar: recomendaciones de mitigación

La seguridad de las API es más importante que nunca desde el punto de vista de la gestión de riesgos y el cumplimiento de las normativas. Sin embargo, debido a la proliferación de API, resulta cada vez más difícil identificar, catalogar y proteger las API del sector de la atención sanitaria. Además, las organizaciones de este sector deben defenderse de los ataques DDoS que amenazan la disponibilidad de los servicios.

No puede defenderse de ataques que no conoce. Por lo tanto, antes de nada debe conocer todos los activos para poder incluirlos en su programa de seguridad. A continuación, necesita saber qué vulnerabilidades existen y tener conocimiento de la situación con respecto a lo que está sucediendo en aspectos como el rendimiento y la seguridad. Por último, es necesario validar la seguridad de los sistemas mediante pruebas de penetración automáticas y clásicas.

Cumplir los siguientes hitos de la estrategia de protección de API y contra ataques DDoS puede ayudarle a lograr un programa de seguridad sólido.

Cinco hitos de la estrategia de protección de API

La adopción de un programa de seguridad de API sólido le ayuda a mejorar la visibilidad de todas sus API y a comprender su exposición al riesgo para que pueda incrementar la protección.

1. Elimine los puntos ciegos de la infraestructura mediante la detección sistemática de las API no autorizadas o en la sombra, y asegúrese de que cada una de ellas se retira o se incorpora en los controles de seguridad de las API.
2. Determine y refuerce la estrategia ante los riesgos mediante el análisis de tipos de alertas comunes y la corrección de defectos en el código de API, la solución de problemas de configuración incorrecta y la implementación de procesos para evitar futuras vulnerabilidades basándose en las lecciones aprendidas.
3. Mejore la detección y la respuesta ante amenazas mediante la comprensión del comportamiento normal y la identificación de posibles abusos según los picos de las alertas de seguridad de API. Posteriormente, incorpore procedimientos de respuesta bien definidos para reducir el volumen de riesgos y alertas a niveles normales.
4. Trabaje con proveedores que ofrezcan formación y experiencia. Deben ofrecer una gama de servicios, desde asistencia basada en proyectos hasta servicios totalmente gestionados que puedan ayudar a configurar y gestionar correctamente soluciones de ciberseguridad complejas e integradas.

La adopción de un programa de seguridad de API sólido le ayuda a mejorar la visibilidad de todas sus API y a comprender su exposición al riesgo para que pueda incrementar la protección.

5. Desarrolle una ofensiva más intensa estableciendo una disciplina formal de búsqueda de amenazas a las API, con el objetivo de identificar posibles amenazas antes de que se materialicen.

Cuatro hitos de la estrategia de protección contra DDoS

Con una situación en la que se baten nuevos récords de ataques DDoS contra API y páginas web de la capa 7, la infraestructura de las capas 3 y 4 y los sistemas DNS, es fundamental garantizar la disponibilidad de sus servicios y funciones. Actualmente, eso significa contar con protecciones activas capaces de hacer frente al tamaño, el alcance y la velocidad de los últimos ataques.

1. Disponer de un sistema que ofrezca visibilidad y respuesta rápida a los ataques. Esto debería incluir protección de la capa 7, las capas 3 y 4 y la infraestructura de DNS.

2. Reforzar su protección frente a DDoS local con una plataforma híbrida de mitigación de ataques DDoS que defienda frente a ataques que sobrecarguen sus dispositivos locales.

3. Recurrir a proveedores o utilizar sistemas que le permitan gestionar fácilmente políticas y mantener listas de autorización de IP, que proporcionen análisis procesables en tiempo real para ayudarle a adoptar una estrategia de seguridad proactiva.

4. Validar las alertas, las funciones de protección y los procesos de gestión de crisis mediante pruebas y asegurándose de que toda su infraestructura cuente con las protecciones adecuadas.

Para obtener más información, lea nuestra investigación más reciente o nuestro blog.

Con una situación en la que se baten nuevos récords de ataques DDoS contra API y páginas web de la capa 7, la infraestructura de las capas 3 y 4 y los sistemas DNS, es fundamental garantizar la disponibilidad de sus servicios y funciones.

Metodología

Ataques DDoS a la capa 7 y a aplicaciones web

Estos datos describen las alertas en la capa de aplicación sobre el tráfico observado a través de nuestro firewall de aplicaciones web (WAF). Las alertas de ataques contra aplicaciones web se activan cuando detectamos una carga maliciosa en una solicitud a un sitio web, una aplicación o una API protegidos. Las alertas DDoS a la capa 7 se activan cuando detectamos anomalías volumétricas en el número de solicitudes a un sitio web, una aplicación o una API protegidos. Estas alertas las pueden activar tanto solicitudes maliciosas como legítimas. Normalmente, son legítimas, pero el gran volumen de solicitudes indica intenciones maliciosas. Las alertas no indican que un ataque haya conseguido su objetivo. Aunque estos productos permiten un alto nivel de personalización, recopilamos los datos presentados aquí de una manera que no tiene en cuenta las configuraciones personalizadas de las propiedades protegidas.

Los datos se extrajeron de una herramienta interna de análisis de eventos de seguridad detectados en Akamai Connected Cloud, una red de aproximadamente 340 000 servidores repartidos entre más de 4000 centros, casi 1300 redes y más de 130 países. Nuestros equipos de seguridad utilizan estos datos, medidos en petabytes mensuales, para investigar ataques, detectar comportamientos maliciosos y proporcionar información adicional a las soluciones de Akamai.

Estos datos cubren el periodo de 18 meses que abarca desde el 1 de enero de 2023 hasta el 30 de junio de 2024.

Actualización de datos de 2024

Nos complace anunciar algunas actualizaciones de nuestros conjuntos de datos para nuestro décimo aniversario. Nuestros conjuntos de datos sobre ataques de bots y a las aplicaciones web han recibido algunas actualizaciones. El método de recopilación de cada uno de ellos se ha transformado, agilizado y optimizado. Además, se ha ampliado el alcance y el nivel de detalle de nuestra perspectiva. Se han agregado clasificaciones para vectores de ataque adicionales, como SSRF. También se ha agregado a cada conjunto de datos la identificación de los ataques dirigidos a los terminales de API. Hemos disfrutado describiendo algunas de estas nuevas mejoras en este informe y nos complace seguir compartiendo estas actualizaciones a lo largo del año (y más adelante) al tiempo que celebramos este hito sobre el estado de Internet en materia de seguridad con nuestros lectores.

Créditos

Director de investigación
Mitch Mayne

Editorial y redacción
Neil Jennings
Chris Notaro
Charlotte Pelliccia
Badette Tribbey
Maria Vlasak
Steve Winterfeld

Revisión y expertos en la materia
Claire Broome
Shane Keats

Análisis de datos
Chelsea Tuttle

Materiales promocionales
Barney Beal

Marketing y publicación
Georgina Morales Hampe
Emily Spinks

Más informes SOTI/ 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 investigaciones 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

Para obtener más información sobre las soluciones de Akamai contra las amenazas dirigidas al sector de la atención sanitaria, visite nuestra **página de sanidad y ciencias de la vida**.