SOTI

10 YEARS
OF SECURITY INSIGHT

Volumen 10,
número 05

Contra viento y marea

Tendencias de ataque a los servicios financieros

Akamai

Estado de Internet / Seguridad

Índice

Introducción

El sector de los servicios financieros no solo representa un pilar de la economía global, sino que también es fundamental para el crecimiento y desarrollo económicos. Los servicios financieros, donde podemos encontrar una amplia gama de segmentos de actividad, como entidades bancarias comerciales, procesadores de pagos, empresas de gestión de activos, bancos de inversión y compañías de seguros, están en constante evolución.

Los avances tecnológicos siguen transformando el panorama de los servicios financieros, generando innovaciones en tecnología financiera (fintech) como bancas digitales, asesores-robot y activos criptográficos. El número de empresas fintech ha aumentado a nivel mundial, siendo Estados Unidos y China los que lideran en este ámbito. En enero de 2024, 8 de las 10 empresas de tecnología financiera más grandes tenían su sede en esos dos países. Este cambio tecnológico también se ve reflejado en el aumento del número de transacciones sin efectivo, que se prevé que aumenten significativamente, sobre todo en lugares donde el acceso a los servicios financieros es limitado. A pesar de ello, sabemos que con la innovación también se produce un aumento de la vulnerabilidad.

Las instituciones financieras son el objetivo constante de los ciberdelincuentes, y las consecuencias de estos ataques van más allá de las pérdidas económicas. Las interrupciones operativas, el daño a la reputación y las devastadoras penalizaciones por no cumplir normativas pueden dañar la base de confianza sobre la que se asienta el sector de los servicios financieros. ¿Cómo pueden las instituciones financieras crear una protección eficaz en un momento en el que el ritmo de la transformación digital solo es comparable a la sofisticación de las ciberamenazas?

Este informe sobre el estado de Internet ayuda a los profesionales de los servicios financieros de todo el mundo (clientes de Akamai, investigadores en materia de ciberseguridad y líderes del sector) a afrontar el panorama de amenazas cada vez más complejo. Como consecuencia de haberse convertido en el principal blanco de los ciberdelincuentes, el sector de los servicios financieros se ve obligado a colaborar para salvaguardar su infraestructura esencial, proteger a las empresas y sus clientes, garantizar la estabilidad de los mercados financieros y evitar estragos económicos. La investigación presentada en este informe es una lectura obligada para quienes desean adelantarse a los atacantes, fortalecer los activos esenciales del sector y garantizar la confianza y fiabilidad continuas que respaldan las relaciones financieras a nivel mundial.

Fortalecimiento de los servicios financieros con cumplimiento, resiliencia operativa y ciberseguridad

Uno de los principales desafíos a los que se enfrenta el sector financiero mundial actualmente es la necesidad de mejorar el cumplimiento y la resiliencia operativa. A medida que el entorno normativo evoluciona, las instituciones financieras deben tomar la iniciativa y adaptarse para responder a estas nuevas exigencias. En la introducción de la Ley de Resiliencia Operativa Digital (DORA), por ejemplo, se subraya la necesidad de contar con un marco sólido capaz de soportar las perturbaciones relacionadas con las tecnologías de la información y la comunicación (TIC). DORA, que entrará en vigor en enero de 2025, exige a las entidades financieras y a sus proveedores de TIC externos que dispongan de estrategias de resiliencia completas, lo que obliga a las empresas a mejorar sus capacidades de respuesta ante incidentes y su seguridad.

En las directrices actualizadas de la Comisión de Bolsa y Valores (SEC) de Estados Unidos se vuelve a subrayar la necesidad de un enfoque de ciberseguridad integral. Las instituciones financieras ahora deben integrar la resiliencia operativa y la recuperación ante desastres en sus estrategias, haciendo hincapié especial en la materialidad de los riesgos cibernéticos. Esto implica tener una idea más clara de cómo las amenazas e incidentes importantes pueden afectar a la estabilidad financiera y a las operaciones. La obligación de comunicar a la mayor brevedad posible los incidentes de ciberseguridad importantes, así como de diseñar de manera meticulosa las estrategias de gestión de riesgos en los informes anuales, supone un cambio de paradigma en las expectativas normativas. Para hacer frente a estos entornos normativos, las instituciones financieras tienen que asociarse con entidades que ofrezcan soluciones de seguridad y visibilidad innovadoras. Como se muestra en este estudio, la experiencia de Akamai puede ayudar a las instituciones de servicios financieros no solo a garantizar el cumplimiento de las normativas, sino también a mantener la integridad operativa en un contexto de estrictos requisitos normativos.

En este contexto, las instituciones financieras deben adoptar un enfoque integral a la hora de abordar los complejos requisitos de cumplimiento y resiliencia operativa, para lo que tendrán que identificar y priorizar los riesgos materiales, aquellos que podrían tener un efecto significativo en el proceso de toma de decisiones de un inversor. Las instituciones financieras deben incorporar estos riesgos materiales en sus marcos de gestión de riesgos y asegurarse de que cuentan con planes fiables de respuesta ante incidentes. El proceso hacia una resiliencia operativa eficaz conlleva la adopción de una estrategia de defensa multicapa en profundidad, con reducción de la superficie de ataque mediante la segmentación y la microsegmentación de la red, la implementación del cifrado de datos en reposo, el refuerzo de los servidores, así como el uso de firewalls de aplicaciones web, junto con sistemas avanzados de detección de amenazas. Una supervisión continua y unas evaluaciones de seguridad periódicas resultan fundamentales para identificar los riesgos y mitigarlos con rapidez.

Los ejercicios de planificación de respuesta ante incidentes, basados en la investigación y la inteligencia contra amenazas actuales sobre la materia, como los informes sobre el estado de Internet (SOTI) de Akamai, son esenciales para las instituciones financieras. Con estos ejercicios se pueden crear escenarios plausibles y se asegura que las instituciones puedan adaptarse a nuevas herramientas, técnicas y procedimientos a medida que vayan surgiendo. Esta estrategia proactiva es esencial para garantizar la resiliencia operativa y mantener la confianza de los clientes en un panorama de amenazas cada vez más volátil. A medida que el sector de los servicios financieros evoluciona, la intersección entre el cumplimiento, la resiliencia operativa y la ciberseguridad seguirá marcando su futuro. Gracias a la adopción de medidas de seguridad avanzadas y a una mejor visibilidad, las instituciones financieras pueden afrontar las complejidades normativas y proteger sus operaciones para conseguir mantener la confianza que resulta tan importante para nuestro negocio.

Teresa Walsh
Responsable a nivel global de Inteligencia del FS-ISAC

Datos clave

34 %

Porcentaje de ataques DDoS a las capas 3 y 4 experimentados por las instituciones de servicios financieros

Los servicios financieros siguen siendo el sector que con más frecuencia es objeto de ataques distribuidos de denegación de servicio (DDoS) en las capas 3 y 4, seguidos del sector de los videojuegos (18 %) y la alta tecnología (15 %). Esta amenaza frecuente probablemente sea resultado de las tensiones geopolíticas actuales, especialmente de las guerras entre Israel y Hamás, así como entre Rusia y Ucrania, que han alimentado un aumento del hacktivismo en todo el mundo.

El aumento del número de API provoca más ataques DDoS a la capa 7

Aunque las aplicaciones web han sido tradicionalmente el principal objetivo de los ciberataques, los ataques DDoS a la capa 7 en las interfaces de programación de aplicaciones (API) han registrado picos destacables durante el periodo analizado. Esto se debe, en gran medida, a la creciente adopción de las API en los servicios financieros para cumplir los requisitos normativos y de conformidad que no paran de cambiar. Los adversarios aprovechan que las organizaciones dependan cada más de las API para adaptar sus tácticas, lo que convierte la seguridad de las API en una prioridad esencial para las empresas modernas.

Los picos de tráfico ponen de manifiesto la necesidad de evaluar la frecuencia y el volumen de los ataques DDoS

Los ataques DDoS a los servicios financieros revelan un dato fundamental: la frecuencia no siempre está correlacionada con la intensidad. Aunque en algunos meses se detectan pocos ataques, los datos correspondientes muestran picos de tráfico significativos, lo que pone de manifiesto la necesidad de tener en cuenta tanto la frecuencia como el volumen al evaluar los efectos de los ataques DDoS.

36 %

Porcentaje de dominios sospechosos dirigidos a instituciones financieras

Los ataques de phishing se dirigen cada vez más a los clientes de servicios financieros, con el consecuente aumento del riesgo de robo de identidades y cuentas. Esta tendencia de ataque hace que haya un mayor escrutinio por parte de los organismos reguladores hacia las instituciones financieras, y que las filtraciones susciten dudas en los clientes en torno a la confianza.

30 %

Porcentaje de visitas a páginas dirigidas a sitios de phishing y de suplantación de marcas

Los atacantes consiguen dirigir el tráfico a sitios fraudulentos que imitan a sitios web y aplicaciones de servicios financieros legítimos. Siguen atacando a las instituciones financieras con phishing para obtener el gran volumen de información confidencial con el que cuentan estas organizaciones.

Los servicios financieros siguen siendo el principal objetivo de los ataques DDoS a las capas 3 y 4

Los ataques distribuidos de denegación de servicio (DDoS) a las capas 3 y 4, las capas de red y transporte, respectivamente, saturan la infraestructura de red y agotan el ancho de banda y los recursos del servidor. Estos ataques envían una gran cantidad de tráfico, con el objetivo de consumir la capacidad de la red y degradar el rendimiento para los usuarios legítimos. De todos los sectores, el de los servicios financieros ha sido el principal objetivo de los ataques DDoS a las capas 3 y 4 (Figura 1). Esta tendencia está motivada por varios factores interconectados que han creado una combinación perfecta de vulnerabilidad y oportunidades para los atacantes.

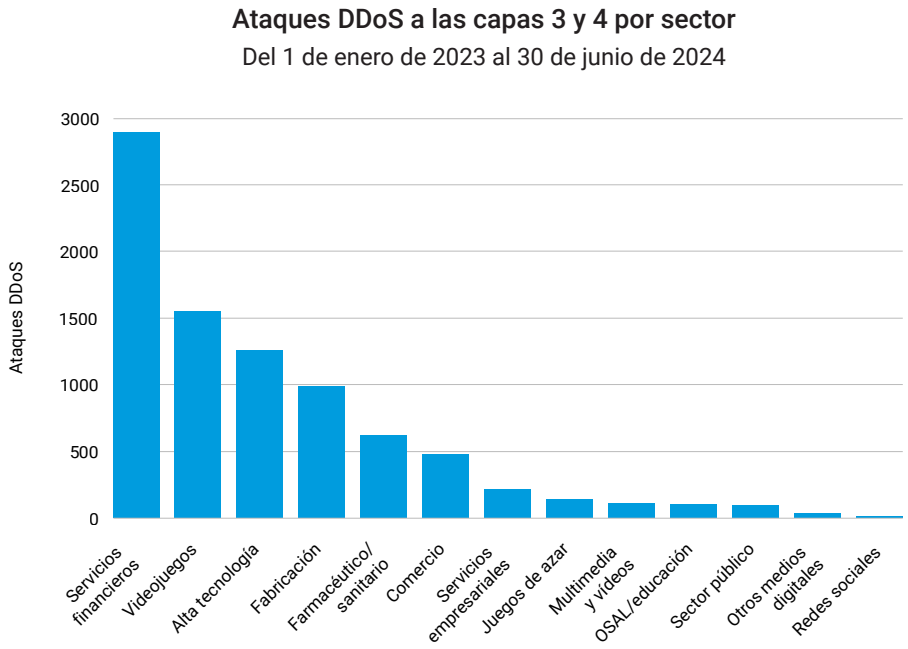


Fig. 1: El sector de los servicios financieros tiene una ventaja destacada respecto a otros sectores que sufren ataques DDoS a las capas 3 y 4

Las tensiones geopolíticas han desempeñado un papel fundamental en el aumento del número de ataques DDoS a las instituciones financieras. La actual guerra entre Rusia y Ucrania, así como la guerra entre Israel y Hamás, han coincidido con destacados aumentos del hacktivismo prorruso y propalestino. Estos conflictos han provocado un auge de los ataques DDoS, especialmente dirigidos contra bancos europeos vinculados a Ucrania. El motivo político que subyace en estos ataques añade un nivel adicional de complejidad al panorama de amenazas.

Las instituciones financieras son objetivos especialmente atractivos para los autores de ataques DDoS debido a todo lo que está en juego. La interrupción de las operaciones puede provocar graves consecuencias financieras, un importante daño a la reputación y una pérdida de confianza en el sistema financiero mundial. El potencial de consecuencias generalizadas convierte a los servicios financieros en un objetivo primordial para aquellos que buscan provocar la máxima perturbación o hacer una declaración política.

Los avances tecnológicos han aumentado considerablemente el poder y la capacidad de los autores de ataques DDoS, que ahora pueden implementar botnets de máquinas virtuales para llevar a cabo ataques de forma más eficaz, al aprovechar los recursos informáticos en numerosas máquinas virtuales y dispositivos del Internet de las cosas (IoT). En esta perspectiva se aprovecha la naturaleza distribuida de los servicios en la nube, lo que dificulta la mitigación y el seguimiento de los ataques. Los atacantes pueden aprovechar el gran ancho de banda disponible y la gran cantidad de recursos informáticos para lanzar ataques DDoS adaptables, potentes y rentables con distintas estrategias.

La creciente superficie de ataque en el sector de los servicios financieros también ha favorecido el aumento de los ataques DDoS. El uso cada vez mayor de servicios digitales y API ha abierto nuevas puertas a los ciberdelincuentes. Este cambio ha aumentado la complejidad de los sistemas financieros y ha hecho posibles numerosas vulnerabilidades nuevas que los atacantes pueden aprovechar. Las API en la sombra no documentadas son un aspecto al que se debe prestar especial atención, ya que no suelen estar protegidas porque los equipos de seguridad de la información no son conscientes de su existencia. Los atacantes pueden aprovechar estas API para exfiltrar datos, eludir controles de autenticación o llevar a cabo acciones disruptivas.

Las presiones normativas han aumentado, de forma involuntaria, la vulnerabilidad de las instituciones financieras frente a los ataques DDoS. Requisitos como la directiva europea sobre servicios de pago, Payment Services Directive 2 (PSD2), introducida por la Unión Europea, han obligado a los bancos a abrir sus sistemas a proveedores externos, como empresas fintech, a través de API. Aunque esto permite a los bancos responder a las cada vez mayores expectativas de los clientes mediante la integración con fintech, aplicaciones móviles y otras plataformas, también aumenta los riesgos de seguridad y amplía la superficie de ataque. El uso adicional de API entre estas diversas entidades crea más puntos de fallo potenciales que se convertirán en los objetivos de los atacantes.

Todos estos factores han contribuido a que el sector de los servicios financieros siga siendo el principal objetivo de los ataques DDoS a las capas 3 y 4. La combinación de motivaciones geopolíticas, objetivos de un gran valor, avances tecnológicos, una mayor presencia digital y presiones normativas han creado un entorno en el que los ataques DDoS a las instituciones financieras no solo son más frecuentes, sino también potencialmente más perjudiciales que nunca. Conforme el sector evoluciona, también lo deben hacer sus defensas contra estas amenazas cada vez más sofisticadas y persistentes.

Los atacantes pueden aprovechar el gran ancho de banda disponible y la gran cantidad de recursos informáticos para lanzar ataques DDoS adaptables, potentes y rentables con distintas estrategias.

Ataques DDoS a las capas 3 y 4: una montaña rusa

Aunque el sector de los servicios financieros es el que sufre la mayor frecuencia de ataques DDoS a las capas 3 y 4, la presencia de estos ataques fluctúa a lo largo del año (Figura 2).

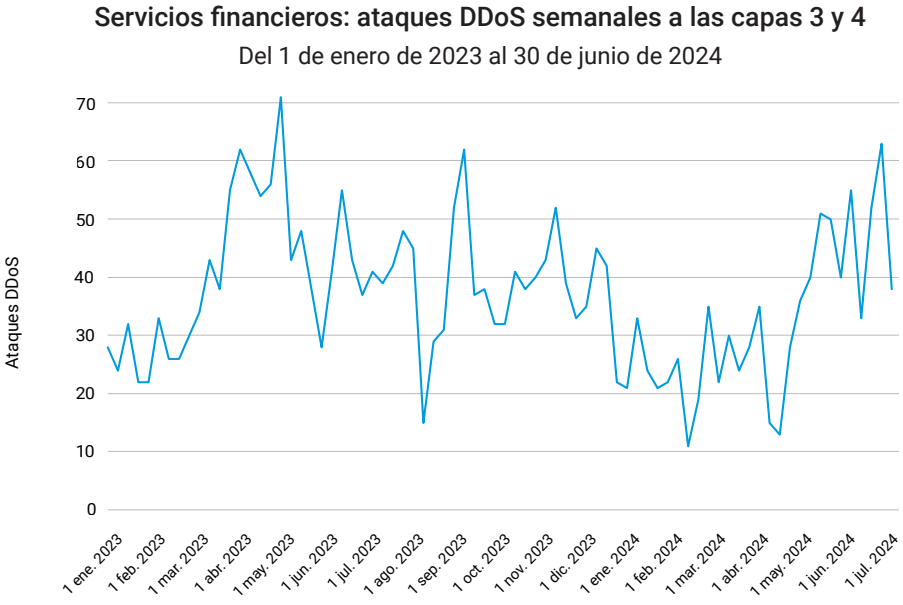


Fig. 2: Patrón de ascenso y descenso de los ataques DDoS a las capas 3 y 4 en el sector de los servicios financieros

Los ataques DDoS a las capas 3 y 4 en el sector de los servicios financieros durante marzo/abril de 2023, agosto/septiembre de 2023 y abril/mayo de 2024 pueden atribuirse a varios factores concretos.

La primavera, de marzo a abril, marca el periodo de impuestos en EE. UU., lo que supone una oportunidad perfecta para los autores de ataques DDoS. Se produjo un aumento notable en la usurpación de cuentas en bancos nacionales y regionales a partir del 16 de abril, fecha que coincide con la época en que muchos bancos comunican sus ganancias del primer trimestre. Durante este periodo, la gestión de acceso e identidades (IAM) y los proveedores de redes, como Okta y Cisco, también notificaron un aumento sustancial y considerable de los ataques de Credential Stuffing dirigidos a servicios online.

En concreto, en abril de 2023, la detección de una vulnerabilidad grave en el protocolo de ubicación de servicios (SLP, por sus siglas en inglés) (CVE-2023-29552) probablemente favoreció el aumento de los ataques. Esta vulnerabilidad, que puede amplificar los ataques DDoS tanto en la capa de red como en la de aplicación, ha afectado a más de 2000 organizaciones de todo el mundo y a más de 54 000 instancias del SLP en Internet. Al aprovechar esta vulnerabilidad, los atacantes podían utilizar las instancias afectadas para iniciar ataques de amplificación de DDoS a gran escala. Con un factor de amplificación de hasta 2200 veces, esta vulnerabilidad permitió uno de los ataques de amplificación más grandes jamás documentados.

Identificamos un ataque clave al examinar el periodo de agosto/septiembre de 2023. Akamai observó y frustró el mayor ataque DDoS registrado contra una institución financiera estadounidense el 5 de septiembre de 2023. En él, se combinaron técnicas de inundación ACK, PUSH, RESET y SYN, alcanzando intensidades máximas de 633,7 gigabits por segundo (Gbps) y 55,1 millones de paquetes por segundo (Mpps). A pesar de su gran intensidad, el ataque fue breve, con una duración menor de dos minutos.

En el punto de mira

Intensidad de los ataques DDoS a las capas 3 y 4: ataques frente a Gbps

Para ser verdaderamente conscientes de la amenaza que los ataques DDoS suponen para el sector de los servicios financieros, es fundamental entender su gran complejidad y escala. No se trata de incidentes simples y aislados, sino que cada ataque suele implicar varios intentos de gran volumen que inundan las redes con gigabits de datos y millones de paquetes por segundo. La sofisticación, intensidad y duración de los ataques están aumentando, y los atacantes utilizan técnicas más variadas, aumentando el riesgo para las instituciones financieras (Figura 3).

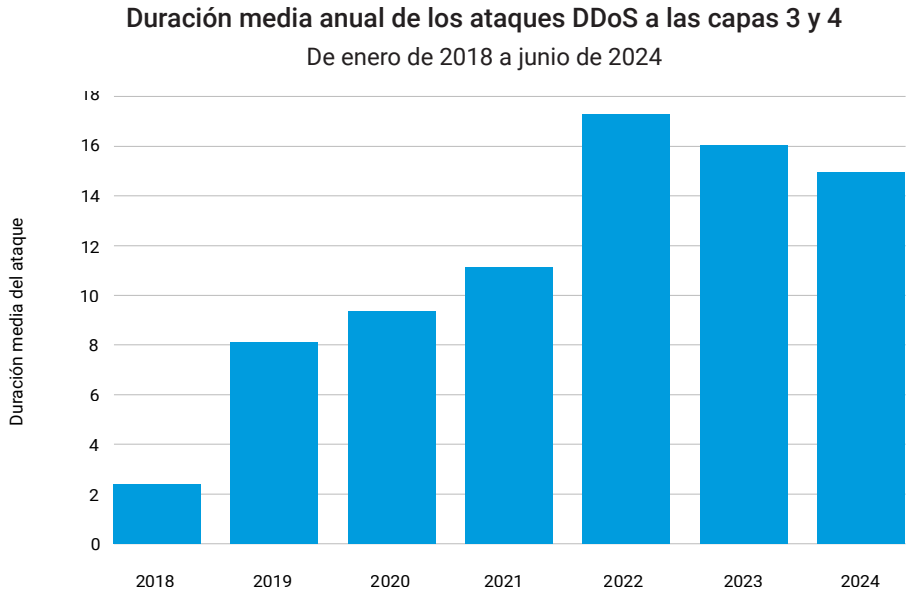


Fig. 3: La tendencia global indica que la duración de los ataques DDoS a las capas 3 y 4 está aumentando

Además, al comparar el gráfico del número de ataques DDoS a las capas 3 y 4 en el sector de los servicios financieros con los datos correspondientes de Gbps de los ataques DDoS, observará una gran discrepancia (Figura 4). En el gráfico de Gbps se observan fuertes aumentos que no se reflejan en el gráfico de ataques. Esta disparidad pone de relieve un concepto importante: incluso un mes con relativamente pocos ataques puede seguir teniendo un volumen extremadamente alto de tráfico DDoS en términos de Gbps.

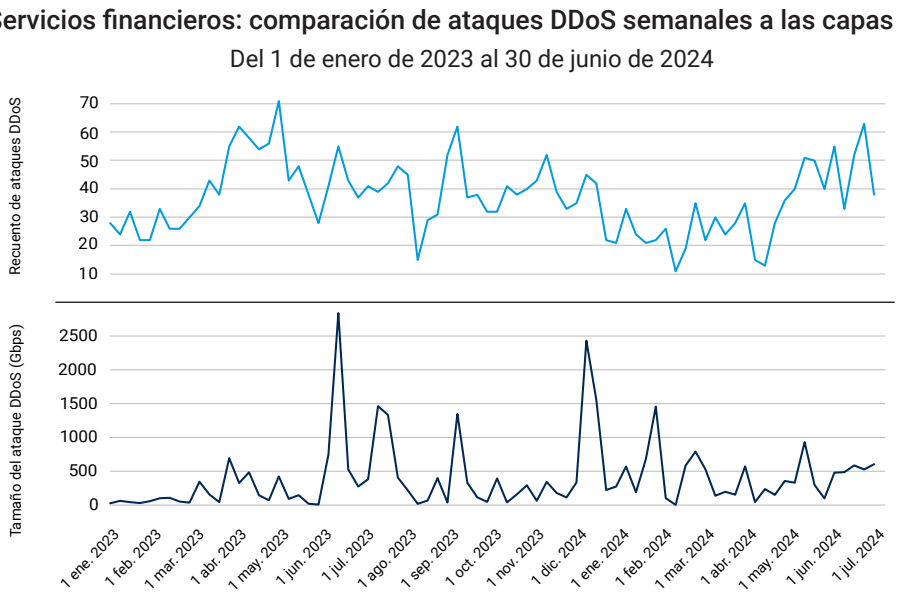


Fig. 4: Ataques DDoS a las capas 3 y 4 del sector de los servicios financieros en comparación con sus mediciones en Gbps

Esta observación destaca un punto crítico: si se confía únicamente en la frecuencia de los ataques se pasa por alto y obvia la verdadera amenaza. Resulta esencial tener en cuenta tanto el volumen como la intensidad del tráfico en cada uno de los ataques. Un reducido número de ataques DDoS de alta intensidad puede provocar mucho más daño que un mayor número de ataques de menor escala, por lo que es imprescindible analizar el alcance de todas las amenazas.

Tendencia a usar uno solo: ataques DDoS en las capas 3 y 4 de un solo vector en los servicios financieros

Los ataques multivectoriales a aplicaciones o redes son una estrategia habitual de los ciberdelincuentes que intentan obtener acceso no autorizado a un sistema o hacer que este falle. Sin embargo, los atacantes centrados en el sector de los servicios financieros parecen intentar usar ataques de un solo vector con mayor frecuencia cuando se trata de ataques DDoS a las capas 3 y 4 (Figura 5).

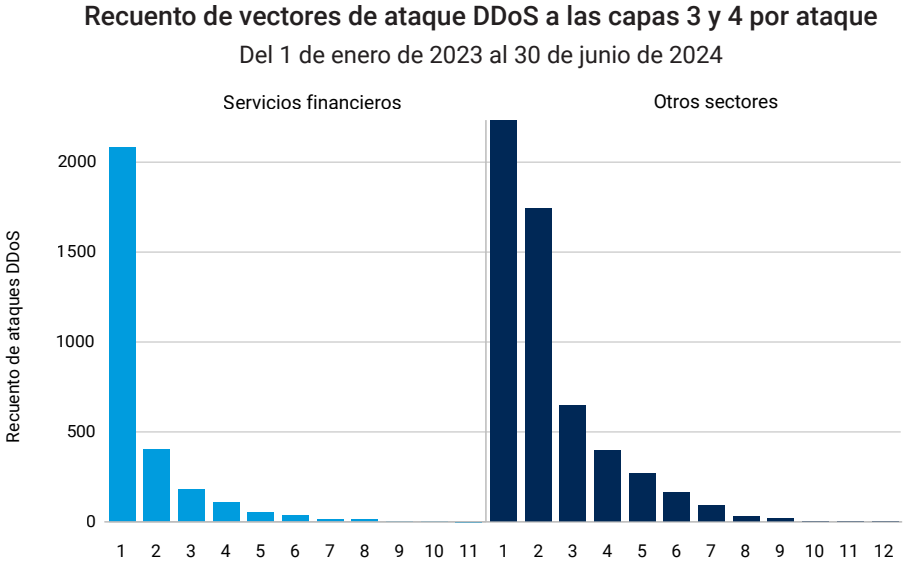


Fig. 5: Los ataques de un solo vector se suelen utilizar más para ataques DDoS a las capas 3 y 4 en el sector de los servicios financieros

Los ataques DDoS de un solo vector contra las capas 3 y 4 requieren menos recursos y pueden ser muy eficaces por sí solos, especialmente contra aquellas instituciones financieras que puedan tener sólidas defensas contra ataques más complejos. Por lo general, son más fáciles de llevar a cabo y requieren menos coordinación que los ataques multivectoriales. También puede haber algunas vulnerabilidades concretas conocidas presentes en las capas 3 y 4 de las instituciones financieras, y que podrían ser el objetivo de un ataque de un solo vector sin el riesgo de probar con otros vectores de ataque que podrían ser detectados por los sistemas de seguridad.

Esta preferencia por los ataques de un solo vector en el sector de los servicios financieros plantea un reto único para los equipos de ciberseguridad. Si bien es necesario mantenerse alerta ante ataques complejos y multivectoriales, resulta crucial asegurarse de que cualquier defensa sea capaz de resistir los ataques de un solo vector que tengan como objetivo las capas 3 y 4.

Aumento de los ataques DDoS a la capa 7 en las API

Los ataques DDoS a la capa de aplicación (capa 7), también conocidos como ataques HTTP o a la capa de tráfico web, son cada vez más frecuentes y se han convertido actualmente en el método preferido de ataque al sector de los servicios financieros. Estos ataques se centran específicamente en los componentes de las aplicaciones que consumen más recursos, lo que impide de hecho el acceso a los usuarios legítimos. A diferencia de los ataques DDoS a las capas 3 y 4, que a menudo se mitigan mediante firewalls y protección de red, los ataques a la capa 7 burlan estas defensas, enmascarándose como solicitudes legítimas cuando van dirigidos a páginas de aplicaciones o funciones de búsqueda específicas, con el objetivo de saturar el servidor de aplicaciones.

Aunque las aplicaciones web del sector de los servicios financieros han sido un objetivo normalmente más frecuente que las API, hemos observado importantes aumentos en el número de ataques DDoS a la capa 7 que tienen como objetivo concreto las API (Figura 6). Estos picos son mucho más significativos y variados que el patrón general de ataque a las API presente en otros sectores.

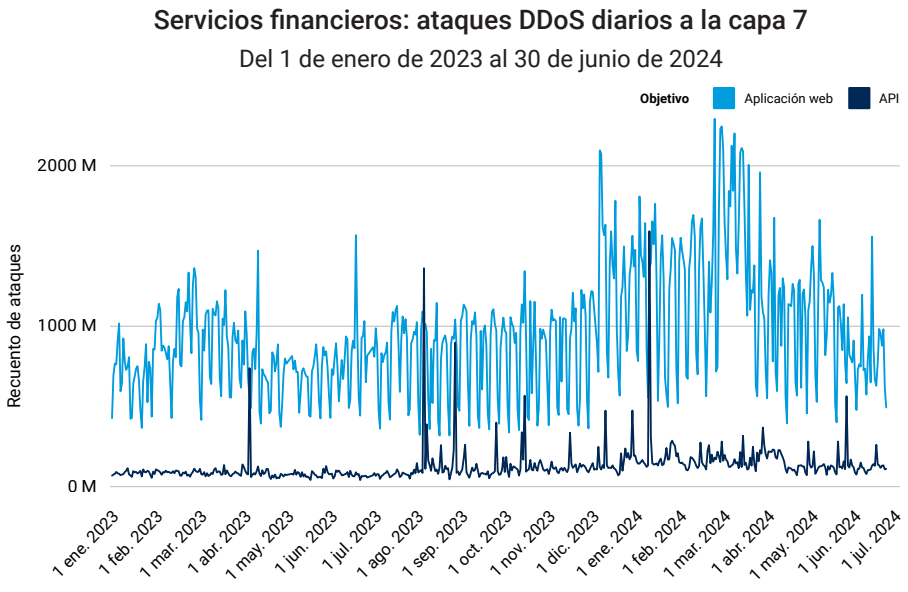
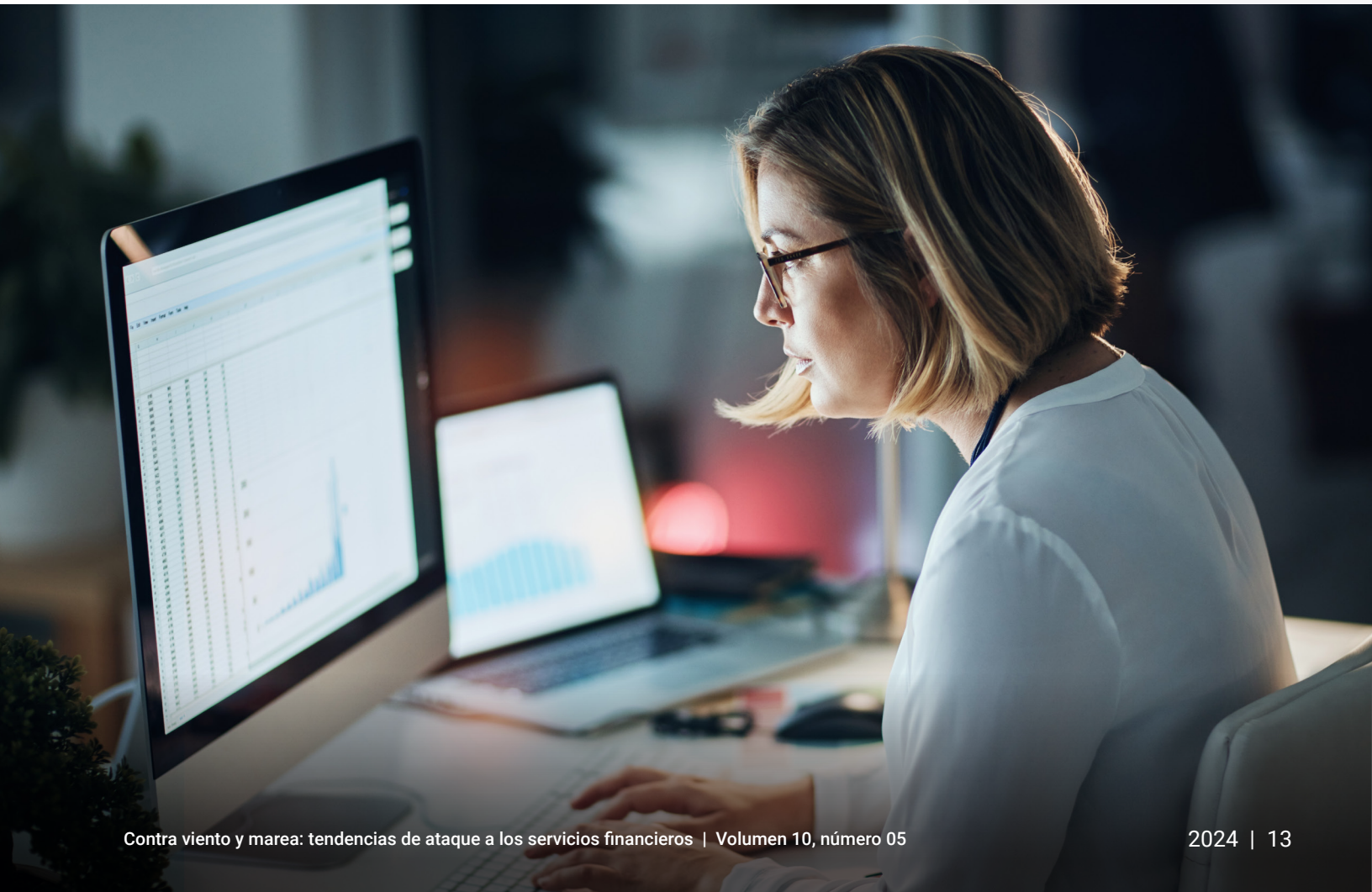


Fig. 6: Los patrones de ataque varían considerablemente en las aplicaciones web y las API objeto de ataques DDoS a la capa 7 en el sector de los servicios financieros

Estos grandes aumentos se produjeron, en concreto, en abril de 2023, agosto de 2023 y enero de 2024. Los atribuimos a factores similares a los que afectan a los ataques a las capas 3 y 4, junto con otros elementos adicionales específicos de la capa 7.

Los atacantes buscan continuamente nuevas vulnerabilidades que explotar, por lo que detectar tales debilidades puede dar lugar a un aumento repentino de la frecuencia de los ataques. Por ejemplo, la vulnerabilidad Rapid Reset en HTTP/2 (CVE-2023-44487), identificada por primera vez en agosto de 2023, posibilitó el lanzamiento de ataques DDoS a la capa 7 que consiguieron los objetivos pretendidos. Esta vulnerabilidad permitió a los atacantes aprovechar una lógica, aparentemente legítima, y agrupar varias solicitudes en un flujo, saturando, de esta forma, los servidores y las aplicaciones. Esto dio lugar al mayor ataque DDoS a la capa 7 registrado hasta la fecha.

Además, los ataques DDoS estacionales siguen siendo una táctica popular para los ciberdelincuentes que atacan a instituciones financieras, con picos importantes durante el periodo fiscal y los periodos festivos. El importante aumento registrado en enero de 2024, tras la ajetreada temporada de compras navideñas, sugiere que los atacantes se estaban preparando para atacar durante periodos de mayor actividad de transacciones online.



Ransomware y hacktivismo en los servicios financieros

El sector de los servicios financieros suele ser objeto de amenazas muy sofisticadas, como los grupos de ransomware. Estos grupos utilizan una amplia gama de técnicas para infiltrarse en instituciones financieras, robar información confidencial y exigir grandes rescates. Aunque las operaciones tienen principalmente motivaciones financieras, también pueden influir los contextos geopolíticos al actuar contra instituciones financieras con posibles vínculos políticos. Este fue el caso del grupo de ransomware con sede en Rusia conocido como REvil (también denominado Sodinokibi). BlackCat (ALPHV) también ha participado en este sentido, como se evidencia en su ataque a un banco importante.

Uno de los grupos de ransomware más activos, conocido por sus ataques contra grandes organizaciones, incluidas las instituciones financieras, sigue siendo LockBit y, todo ello, a pesar de las recientes acciones de las fuerzas del orden contra el grupo. La operación Cronos, en la que colaboraron Europol y Eurojust para coordinar un grupo de trabajo internacional pionero, se ha visto superada por la nueva infraestructura puesta en marcha por LockBit. El grupo de ransomware resurgió con una nueva infraestructura y un sitio de filtración en la Dark Web pocos días después de que, tras la operación de las fuerzas del orden, se confiscaran sus servidores en febrero de 2024. Además, LockBit ha declarado que respondería a la operación Cronos aumentando el número de ataques a las redes gubernamentales.

El grupo de ransomware CL0P también sigue activo y es especialmente conocido por aprovechar las vulnerabilidades del software de transferencia de archivos muy utilizado en organizaciones, incluidas las instituciones financieras. Un ejemplo destacado fue la vulnerabilidad de día cero CVE-2023-34362, que afectó al software MOVEit Transfer y que comenzó con una inyección SQL para infiltrarse en dicha aplicación web. Al menos 15 bancos y cooperativas de crédito confirmaron filtraciones de datos como resultado de la vulnerabilidad en MOVEit. CL0P también ha obtenido acceso inicial mediante otras técnicas, como el phishing, además de seguir ejecutándose como modelo de ransomware como servicio (RaaS). Recientemente, el grupo ha mejorado sus tácticas para emplear la extorsión cuádruple en objetivos como las instituciones financieras. Además de las técnicas usadas en la extorsión triple, la extorsión cuádruple incluye el envío de mensajes para acosar a partners comerciales, empleados, clientes, ejecutivos de alto nivel y medios de comunicación para informarles de que la organización ha sido pirateada. Y esta estrategia ha provocado un incremento del importe medio de pago en un rescate de ransomware.

Otros hacktivistas que tienen como objetivo las instituciones financieras, pero que no están considerados grupos de ransomware, son Anonymous Sudan, KillNet y NoName057(16). Todos ellos son conocidos por sus actividades relacionadas con la guerra entre Rusia y Ucrania. Además, Anonymous Sudan también ha afirmado haber participado en ciberataques como respuesta a la guerra entre Israel y Hamás. El año pasado, estos grupos, además de muchos otros grupos de atacantes, aprovecharon el caos provocado por la guerra entre Rusia y Ucrania, y centraron su atención en la infraestructura bancaria esencial.

Hay muchos otros prolíficos atacantes que no están considerados grupos de ransomware, pero que son conocidos por atentar contra el sector de los servicios financieros, como Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt y APT41.

Dadas las amenazas actuales que plantean estos actores, resulta fundamental que las instituciones financieras sean conscientes del panorama actual de amenazas y conozcan mejor las motivaciones y técnicas que usan los atacantes para desarrollar estrategias de defensa más eficaces. Consulte nuestra sección sobre mitigación, que aparece más adelante en este informe, para conocer las medidas de protección recomendadas.

Reciente brote de hacktivismo DDoS golpea a las instituciones financieras de Oriente Medio

El sector de los servicios financieros de Oriente Medio ha experimentado últimamente un aumento sostenido de sofisticados ataques DDoS derivados de las tensiones geopolíticas. Esta tendencia es especialmente frecuente en la región de Europa, Oriente Medio y África (EMEA) y es un ejemplo de la creciente amenaza que representan los ataques DDoS con motivación política contra las instituciones financieras.

Un ejemplo destacado de esta tendencia se produjo a comienzos de este año, cuando BlackMeta (también conocido como DarkMeta), grupo hacktivista propalestino, lanzó un ataque DDoS a la capa 7 de seis días contra una institución financiera de los Emiratos Árabes Unidos (EAU). El ataque fue posible gracias a InfraShutdown, servicio de DDoS de alquiler, lo que pone de manifiesto la creciente accesibilidad de estas herramientas de ataque. El grupo BlackMeta, que ha estado activo desde noviembre de 2023, tiene un historial de ataques a organizaciones de Israel, los EAU y Estados Unidos.

El ataque a la institución financiera de los EAU fue significativo tanto en duración como en intensidad. Duró aproximadamente 100 horas, con unas ondas de solicitudes web que duraron entre 4 y 20 horas, y con una media de 4,5 millones de solicitudes por segundo. El ataque tuvo al banco bajo fuego el 70 % del tiempo, lo que afectó de manera importante a sus servicios. La campaña de BlackMeta contra el banco formó parte de una iniciativa más amplia de protesta contra las injusticias percibidas contra palestinos y musulmanes, y en ella se vieron tácticas similares a las empleadas por Anonymous Sudan.

Afortunadamente, las medidas de mitigación de la institución financiera impidieron interrupciones más graves, pero este incidente subraya la tendencia al alza de los ciberataques con motivaciones políticas. También destaca la creciente disponibilidad de los servicios de DDoS de alquiler, que bajan el listón para que los grupos de hacktivistas lancen ataques a gran escala. Este avance destaca la necesidad de contar con medidas sólidas de ciberseguridad para ofrecer protección contra amenazas persistentes y de gran volumen.

El 15 de julio de 2024 se produjo otro ataque DDoS, con presunta motivación política, a una importante empresa de servicios financieros de Israel. Este ataque masivo, originado en una botnet globalmente distribuida, duró casi 24 horas y alcanzó un máximo de 798 Gbps. Akamai consiguió mitigar este ataque DDoS a las capas 3 y 4, que incluía varios vectores, como la reflexión DNS y la inundación UDP.

Durante este ataque, Akamai bloqueó aproximadamente 389 terabytes de tráfico malicioso en una fase intensiva de tres horas, con un total de tráfico bloqueado de aproximadamente 419 terabytes mientras estuvo activo. La presencia de otras interrupciones a las que tuvieron que hacer frente las instituciones financieras israelíes el mismo día sugiere un ataque coordinado, lo que pone de relieve la creciente amenaza que plantean los ataques DDoS avanzados.

Es importante destacar que este agresor, con muchos recursos, había atacado previamente a otro cliente de servicios financieros 27 veces en los últimos 90 días. El cliente ha sido objeto de ataques DDoS reiterados desde el cuarto trimestre de 2023, coincidiendo con la guerra entre Israel y Hamás. El grupo interno de Akamai de inteligencia contra amenazas DDoS informa de que las instituciones y empresas de Israel han experimentado un número sin precedentes de ataques DDoS en 2024. Esta campaña sostenida y agresiva pone de manifiesto el creciente alcance e intensidad de estas amenazas, dejando claro que los atacantes son cada vez más persistentes y cuentan con más recursos.

Confiar en lo conocido: abuso de marca en los servicios financieros

A medida que los servicios financieros adoptan enfoques centrados en la digitalización para mejorar la experiencia del cliente, la eficiencia operativa, la innovación, los ingresos generales y la visibilidad, los ciberadversarios se aprovechan de la confianza inherente que existe entre las organizaciones y sus clientes a través de esquemas de suplantación de la marca. En la Figura 7 se muestran ejemplos de sitios fraudulentos que imitan a instituciones financieras conocidas. Si bien el phishing y la suplantación de marca son métodos de uso habitual, el alarmante número de sitios web fraudulentos y el rápido ritmo con el que los atacantes pueden crear dominios una vez que sus sitios originales se desconectan son especialmente preocupantes. Esta rápida proliferación plantea una amenaza creciente e incesante para el sector de los servicios financieros.

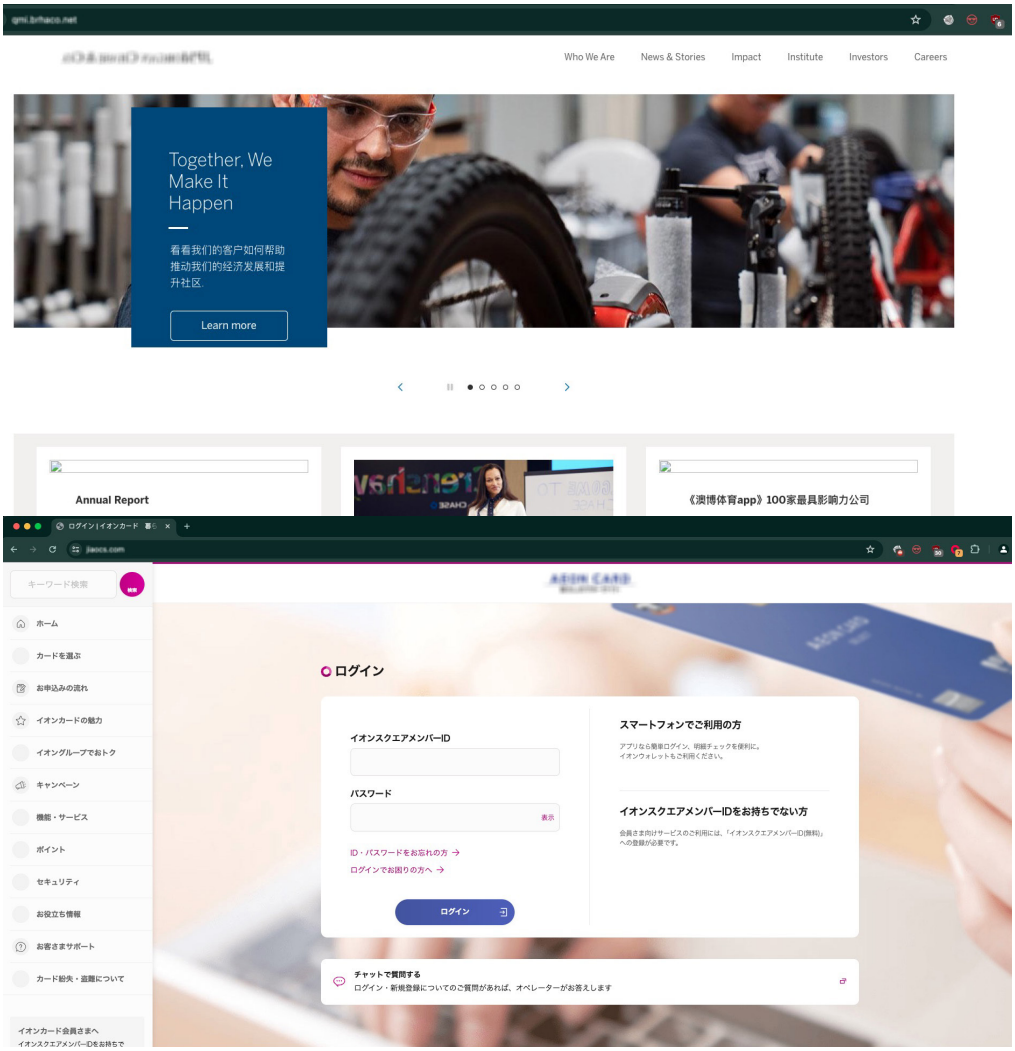


Fig. 7: Ejemplos de sitios fraudulentos de phishing que imitan a conocidas instituciones financieras

El panorama del abuso de marca se ha visto alterado significativamente por la aparición de plataformas y kits de herramientas de phishing como servicio. Estos recursos han facilitado la entrada de los ciberdelincuentes, lo que ha afectado drásticamente a la magnitud y escala de los ataques de phishing contra los servicios financieros y sus clientes. Para poner esto en perspectiva, el Grupo de Trabajo Antiphishing (APWG) registró casi cinco millones de ataques de phishing en 2023, designándolo como "el peor año de phishing registrado".

El abuso de marca puede suponer un impulso para riesgos cada vez mayores, como el robo de identidad y la usurpación de cuentas. Los atacantes a menudo venden información sobre los clientes en la Dark Web o la utilizan para llevar a cabo el robo de cuentas. Desde el punto de vista de la seguridad, una intervención temprana en los ataques a la marca resulta fundamental. Al frustrar el ciclo de vida del ataque desde el principio, puede evitar que los atacantes recopilen credenciales con fines malintencionados.

Los riesgos del abuso de marca van más allá de las preocupaciones por problemas inmediatos en materia de seguridad. Una organización puede sufrir pérdidas financieras considerables debido a daños en la reputación, problemas legales y de cumplimiento, e incluso pérdidas de ventas debido a la falsificación de productos. En el panorama digital actual, la detección temprana de los ataques de suplantación de marca es fundamental para mantener la confianza de los clientes y la continuidad empresarial.

Argumento de engaño: análisis detallado de los ataques de suplantación

Los equipos de seguridad se enfrentan al enorme desafío de defenderse del abuso de marca que puede producirse en varias plataformas online, lo que hace que sea difícil proteger los activos digitales, ya que tanto los usuarios legítimos como los atacantes pueden acceder a ellos. A menudo, los atacantes extraen el contenido de activos públicos, como los portales de banca online, para crear su propio sitio web falsificado y registrar un dominio con un nombre casi idéntico al de la entidad real para engañar a los usuarios desprevenidos. Además, los ciberadversarios lanzan campañas que incluyen correos electrónicos de phishing, publicaciones en redes sociales y otros canales digitales para atraer a las posibles víctimas a sus sitios maliciosos o a aplicaciones falsas.

Para realizar este informe, analizamos las actividades de suplantación de identidad de marca y phishing observadas en los dominios activos en los últimos 12 meses para proporcionar información sobre la prevalencia de la suplantación de marca en los distintos sectores, con especial atención en los servicios financieros. La visibilidad total y la solución patentada de Akamai nos permiten:

- realizar un seguimiento del tráfico presente en sitios de phishing y suplantación de marcas, incluyendo mercados;
- identificar el número de dominios maliciosos activos, y
- asignar puntuaciones de gravedad a los dominios maliciosos.

Los servicios financieros fueron el sector más suplantado (36,25 %) entre todos los sitios sospechosos que Akamai supervisó (Figura 8). Este resultado pone de relieve especialmente la vulnerabilidad del sector de los servicios financieros a la suplantación y el abuso de marcas. Las organizaciones de los sectores del comercio (26,41 %) y de los servicios empresariales (18,90 %) ocuparon el segundo y tercer puesto, respectivamente.

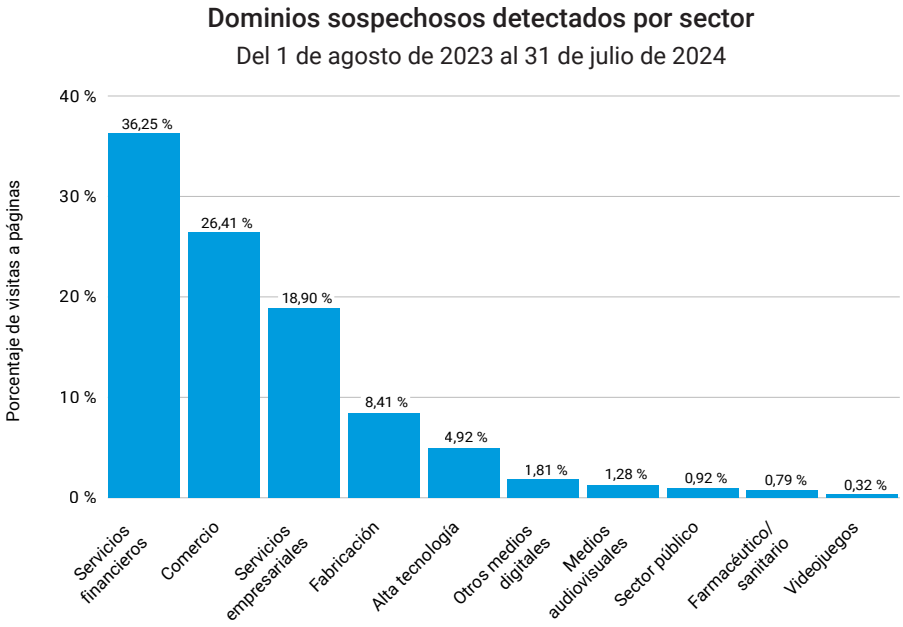


Fig. 8: Los servicios financieros representaron el 36,3 % de los dominios de suplantación de identidad de marca o phishing

El sector de los servicios financieros es uno de los principales objetivos de los ataques de suplantación de marca debido a la enorme cantidad de datos confidenciales y de gran valor que posee, como credenciales bancarias e información de identificación personal (PII). La información obtenida de sitios bancarios falsificados permite a los ciberdelincuentes acceder fácilmente a las cuentas y, posteriormente, vaciarlas. También se pueden obtener otros datos financieros de gran valor, como credenciales de carteras electrónicas y cuentas de criptomonedas (los precios oscilan entre 120 dólares y 400 dólares en la Dark Web), lo que permite a los atacantes transferir lo que hay en la cuenta o vender la información en mercados oscuros. La alta rentabilidad de estos esquemas convierte a los servicios financieros en objetivos principales de los ataques de phishing y abuso de marca.

Del mismo modo, las empresas que hacen venta al público en general se han convertido en objetivos lucrativos del abuso de marca desde el auge del comercio electrónico y las compras online, lo que ofrece oportunidades para obtener credenciales, así como otro tipo de información personal. Las empresas fabricantes y los proveedores externos que ofrecen servicios son igualmente vulnerables al abuso de marca. Aunque la digitalización favorece el crecimiento general de la empresa, se ha convertido en un punto débil vulnerable para muchas organizaciones, lo que ha provocado la proliferación de ataques de suplantación de identidad de marca y un aumento de los intentos de phishing.

La alta rentabilidad de los esquemas [de suplantación de marca] convierten a los servicios financieros en objetivos principales de abuso de marca y ataques de phishing.

Las organizaciones deben mantenerse alerta e implementar medidas de seguridad para proteger tanto a las marcas como a los clientes en este panorama digital en constante evolución. Para ello, deben supervisar de forma continua el uso indebido de la marca, llevar a cabo procedimientos rápidos de neutralización de sitios fraudulentos e informar a los clientes para que reconozcan los posibles intentos de suplantación. Al priorizar estas iniciativas, las organizaciones pueden proteger mejor su reputación y la confianza de sus clientes en un entorno de amenazas cada vez más complejo.

Servicios financieros en el punto de mira del abuso de marca

Para obtener una visión integral del impacto de la suplantación de la marca y el phishing, también hemos analizado el número de visitas a páginas web sospechosas. Nuestros resultados revelan que los sitios que se enmascaran como instituciones financieras recibieron el 30 % de las visitas, mientras que los que imitan a empresas de comercio aparecían a continuación con el 20 % de las visitas (Figura 9). Estos resultados sitúan sistemáticamente a los servicios financieros y el comercio en los primeros puestos, tanto si medimos por solicitudes como por dominios. Esta constancia pone de manifiesto su posición como objetivos principales del abuso y la suplantación de marca, y por una buena razón.

Los servicios financieros abarcan una amplia gama de objetivos, desde bancos muy consolidados hasta instituciones más pequeñas con menos recursos de seguridad, todos ellos con un gran nivel de riesgo. El comercio, otro sector sometido a un escrutinio similar por parte de los foros de cumplimiento (por ejemplo, el Consejo de Normas de Seguridad del Sector de las Tarjetas de Pago) como el de los servicios, también tiene que asumir importantes riesgos debido a la gran cantidad de información que poseen de los clientes.

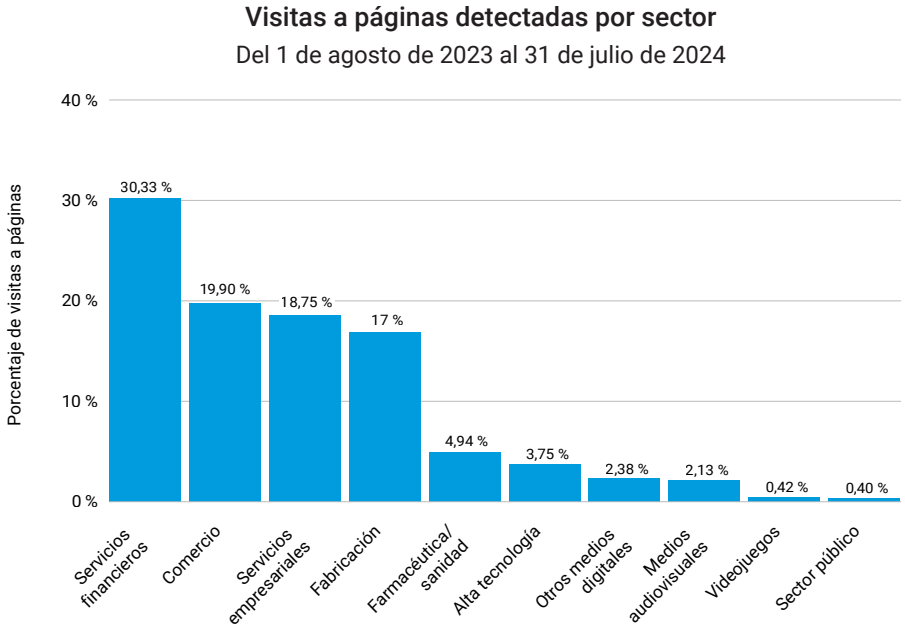


Fig. 9: Más del 30 % de las visitas a páginas durante el periodo del informe (de agosto de 2023 a julio de 2024) se produjeron en sitios sospechosos que se enmascaraban como sitios legítimos de servicios financieros

Curiosamente, observamos algunas disparidades entre las clasificaciones de suplantación de dominios y las cifras reales de visitas en todos los sectores. Por ejemplo, la alta tecnología se sitúa entre los cinco primeros en cuanto a dominios suplantados, pero cae hasta el sexto puesto en términos de visitas reales. Del mismo modo, hay menos dominios que se hacen pasar por dominios farmacéuticos/sanitarios, pero estos dominios tienen más visitas.

Phishing para obtener credenciales

El abuso de marca adopta muchas formas, entre ellas sitios similares que replican el logotipo y el diseño exactos de la empresa legítima, aplicaciones fraudulentas y perfiles falsos de redes sociales que imitan a las cuentas corporativas oficiales. Para comprender plenamente este problema, analizamos las páginas falsificadas y las clasificamos por tipos: suplantación de marca, phishing, aplicaciones no autorizadas, tiendas falsas, elementos que eluden las barreras de pago, así como tiendas falsas y perfiles falsos en redes sociales. Es importante tener en cuenta que el dominio de una sola organización puede incluirse en varias clasificaciones según las páginas que supervisamos.

Nuestro análisis puso de manifiesto que el phishing es el método más usado en los dominios falsificados que tienen como objetivo a instituciones de servicios financieros, lo que representa un asombroso 68 % de todas las instancias registradas (Figura 10). En segundo lugar se encuentra la suplantación de marca, ya que suma el 24 % de todos los dominios registrados. Entre los sitios más frecuentados por los usuarios, el phishing y la suplantación de marca vuelven a ocupar el primer y segundo lugar, respectivamente. Otros métodos de abuso de marca, como las tiendas y los perfiles falsos en redes sociales son menos importantes en las instituciones financieras que en otros sectores. A pesar de que hay menos ataques que tengan como objeto aplicaciones vulnerables, es importante tener en cuenta que los atacantes están adoptando métodos cada vez más creativos para ampliar su campo de acción.

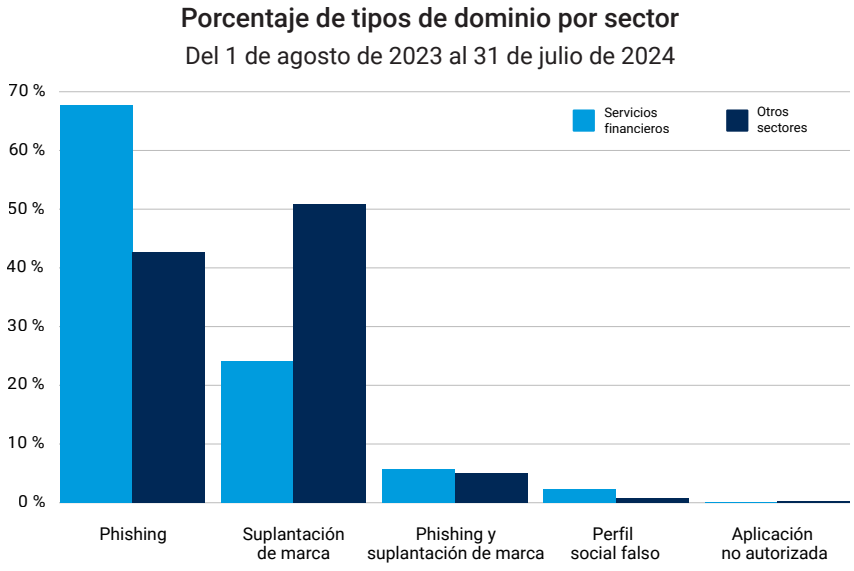


Fig. 10: La mayoría de los dominios que registramos para los servicios financieros son sitios web de phishing, que incluso superan el total del resto de sectores en su conjunto

Las instituciones financieras se consideran entidades que generan mucha confianza, lo que las convierte en el objetivo principal de los estafadores que se aprovechan de esa confianza.

A pesar de la mayor conciencia de los riesgos que plantea el phishing, el elemento humano sigue siendo una brecha de seguridad considerable, que se ve agravada por las sofisticadas técnicas que utilizan los atacantes (consulte la sección La anatomía del abuso de marca para obtener más información), lo que dificulta para los no expertos la detección de una página falsa. Las instituciones financieras se consideran entidades que generan mucha confianza, lo que las convierte en el objetivo principal de los estafadores que se aprovechan de esa confianza. Al suplantar a estas instituciones, los atacantes engañan a los usuarios para que entreguen voluntariamente sus credenciales, aprovechando la reputación de la institución para que sus estafas sean más convincentes y eficaces.

Para proteger tanto a una organización como a sus clientes, es fundamental utilizar tecnologías de seguridad con funciones de supervisión de marca capaces de controlar de forma proactiva cualquier uso no autorizado de la misma, ya sea un nombre de dominio, una aplicación móvil o una comunicación por correo electrónico. Una vez identificados, el siguiente paso consiste en poner en práctica las medidas necesarias para impedir el tráfico, que podría exponer a los clientes a los peligros (como el robo de datos) que plantean el abuso de marca y el phishing.

Caso real: creciente sofisticación de los ataques de Credential Stuffing contra instituciones financieras

Una empresa estadounidense de tecnología financiera soportó ataques constantes de Credential Stuffing a lo largo de los años 2023 y 2024 contra una de sus aplicaciones orientadas al cliente. La magnitud de estos ataques es asombrosa: durante un periodo de 24 horas, Akamai detectó más de 3000 alertas de diferentes direcciones IP que intentaban infiltrarse en cuentas con credenciales robadas. Observamos que una sola dirección IP intentaba al menos 115 combinaciones de nombre de usuario y contraseña. En total, registramos más de 100 000 alertas en julio de 2024.

Sitios de servicios financieros fraudulentos con nivel de riesgo crítico

Nuestra inteligencia exclusiva a nivel mundial, combinada con fuentes de datos adicionales de inteligencia contra amenazas de terceros, nos aporta una clara ventaja a la hora de detectar suplantaciones de marcas. Utilizamos este completo sistema para examinar y clasificar de forma meticulosa cada dominio en función de su puntuación de amenaza.

Calculamos la puntuación de la amenaza utilizando tres factores clave:

1. **La puntuación de confianza**: nuestra certeza de que un evento es un intento de phishing.
2. **El nivel de gravedad**: el grado de riesgo (crítico, alto, medio o bajo) asociado a un evento.
3. **El factor de frecuencia**: el número de eventos/sesiones asociados al sitio en un intervalo de tiempo concreto.

Nuestro sistema de puntuación pondera los tres factores clave: confianza, gravedad y frecuencia. Combinamos estas puntuaciones para generar una puntuación de amenaza completa para cada dominio sospechoso, con un límite de 99, a fin de garantizar una evaluación integral de las posibles amenazas.

Nuestro análisis más reciente revela que el sector de los servicios financieros tiene una alarmante puntuación promedio de amenaza de 85, lo que pone de relieve los graves riesgos a los que se sigue enfrentando (Figura 11). Esta puntuación coloca a las instituciones financieras de lleno en el punto de mira de los ciberdelincuentes, que tienen como objetivo constante a sus grandes almacenes de información confidencial.

Puntuaciones de amenazas por sector

Sector	Puntuación promedio de amenaza	Sector	Puntuación promedio de amenaza
Sector público	**95**	Videojuegos	**65**
Servicios financieros	**85**	Fabricación	**64**
Servicios empresariales	**85**	Otros medios digitales	**62**
Farmacéutico/sanitario	**85**	Comercio	**61**
Medios audiovisuales	**71**	Alta tecnología	**60**

Fig. 11: En nuestro cálculo de las puntuaciones promedio de amenazas se observa que los servicios financieros tienen una puntuación alarmantemente elevada

Aunque el sector público registró la puntuación promedio más alta de amenaza, probablemente debido a su gran cantidad de información confidencial y a los limitados recursos de seguridad, los servicios financieros siguen siendo un objetivo igualmente atractivo, donde los atacantes se ven atraídos por la posibilidad de obtener enormes beneficios económicos. Sectores como el de los servicios empresariales y el farmacéutico y sanitario también obtienen unas puntuaciones similares, lo que indica que los ciberdelincuentes están diversificando sus objetivos, pero las instituciones financieras siguen siendo un objetivo prioritario debido a la naturaleza esencial de sus datos.

Este alto nivel de amenaza exige que se adopten medidas de inmediato para fortalecer las defensas y mitigar las amenazas en constante evolución antes de que causen daños financieros y a la reputación importantes.

La anatomía del abuso de marca

El éxito del fraude y el abuso de marca dependen, en gran medida, del potencial de la marca como cebo de ingeniería social. Los atacantes aprovechan la sensación de familiaridad y confianza inherente que tienen los consumidores con respecto a las marcas conocidas para diseñar sitios web falsos que imitan muy bien a los legítimos. En algunos casos, los estafadores incluso copian el código exacto, lo que hace que estos sitios ilegítimos parezcan casi idénticos a los reales. Con el aumento de las herramientas de IA generativa, que ayudan a los estafadores a detectar errores ortográficos y gramaticales, a los consumidores les resulta aún más difícil distinguir entre sitios auténticos y falsos.

La magnitud de las campañas de phishing y suplantación se ve acrecentada por la existencia de kits de herramientas de phishing. Por tan solo 50 dólares, los atacantes pueden adquirir estos kits de herramientas y crear sitios de phishing convincentes. La labor del ciberdelincuente de desarrollar, crear y vender kits de herramientas de phishing reduce significativamente la barrera de entrada para llevar a cabo campañas de phishing y suplantación. Kr3pto y 16Shop son dos ejemplos de kits de herramientas de phishing habituales. Kr3pto dirigió sus ataques contra bancos del Reino Unido omitiendo la autenticación de dos factores, mientras que 16Shop se centró en marcas importantes como PayPal y Amazon, entre otras. En agosto de 2023, como resultado de una operación policial internacional, se produjo la detención de los creadores de 16Shop. Estos casos ponen de relieve la sofisticación en constante evolución de los ataques de phishing y los esfuerzos conjuntos para combatir la ciberdelincuencia.

La magnitud de las campañas de phishing y suplantación se ve acrecentada por la existencia de kits de herramientas de phishing.

Infravalorado pero eficaz: combosquatting

Otro aspecto importante del abuso de marca es el uso de nombres de dominio que se asemejan mucho a los sitios web legítimos. Normalmente, los atacantes registran sus dominios después de comprar o crear su propio sitio de phishing. Aquí es donde las técnicas de eficacia probada, como el cybersquatting y sus numerosas variantes, desempeñan un papel fundamental. Una táctica común es el typosquatting, en el que los atacantes registran un dominio con un ligero error ortográfico en el nombre de una empresa (por ejemplo, acamai[.]com), con la esperanza de que el consumidor cometa un error tipográfico. Otro método, el combosquatting, consiste en añadir palabras clave adicionales (como "support", "login" o "help") al nombre de dominio. Esta táctica utiliza los micrositios que se suelen encontrar en los sitios web legítimos de la empresa.

Según las investigaciones de Akamai, a pesar de ser una táctica de la que se informa poco, el comboquatting (la adición de una palabra clave) supera al typosquatting (la adición, eliminación o sustitución de un carácter) en el número de dominios activos. Curiosamente, "com" surgió como una de las principales palabras clave añadidas en los sitios fraudulentos.

Mecanismo de distribución

Los sitios web falsificados y de phishing se distribuyen y atraen a sus víctimas a través de diversos mecanismos, siendo el correo electrónico el principal de ellos. Estos correos electrónicos parecen convincentes porque usan un logotipo legítimo y contienen mensajes urgentes, como solicitudes para actualizar la información de la cuenta. Sin embargo, el abuso de marca no se limita a los sitios web y los correos electrónicos: los atacantes también propagan amenazas a través de las redes sociales, con lo que pueden llegar más lejos tanto ellos como sus tácticas de engaño.

(Enlaces) ocultos a la vista

Existen otras tácticas observadas en circulación que dificultan a los consumidores la identificación de un sitio de suplantación y que pueden aumentar el índice de éxito de estos ataques. Por ejemplo, el uso de URL acortadas, códigos QR, hipervínculos de imágenes y enlaces de texto en SMS que ocultan los enlaces maliciosos. A diferencia del correo electrónico, donde filtros de correo no deseado proporcionan protección contra este abuso, es probable que las estafas de texto no se bloqueen y tengan una mayor probabilidad de leerse o abrirse.

Existen otras tácticas observadas en circulación que dificultan a los consumidores la identificación de un sitio de suplantación y que pueden aumentar el índice de éxito de estos ataques.

Ataques regionales de phishing y suplantación de marca en los servicios financieros

El abuso de marca afecta a organizaciones y consumidores de todo el mundo, pero algunas regiones experimentan un mayor nivel de vulnerabilidad al fraude y el abuso debido a la concentración del tráfico en sitios de suplantación de marca y phishing. Nuestro análisis revela que la región de EMEA experimentó el mayor volumen de tráfico a sitios de phishing y suplantación detectados en los últimos 12 meses, incluso superando a los de Norteamérica (Figura 12). En esta clasificación se incluyen tanto los servicios financieros como otros sectores.

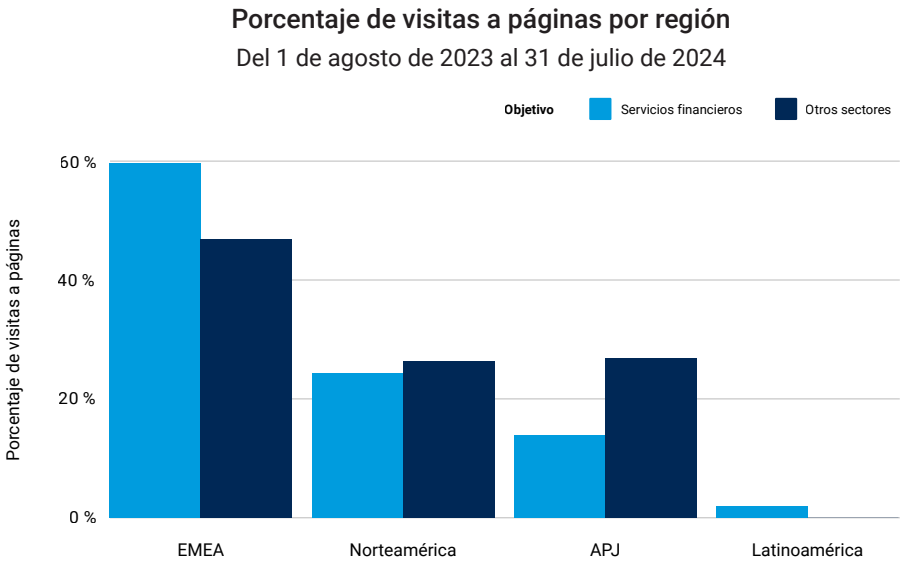
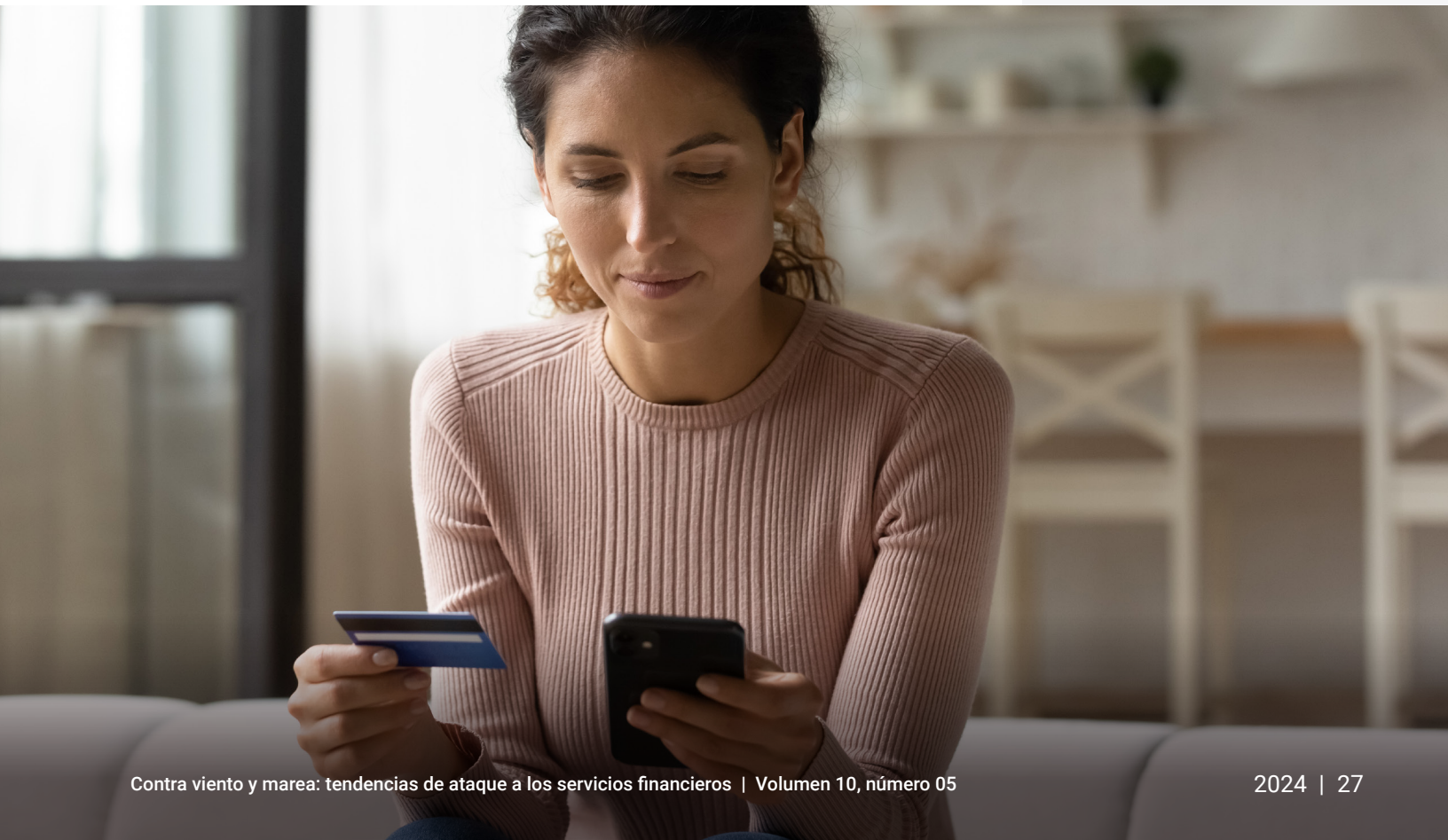


Fig. 12: EMEA superó a Norteamérica como región más afectada por el phishing y el abuso de marca en los servicios financieros

Aunque las regiones de América Latina y Asia-Pacífico y Japón (APJ) registraron cifras relativamente menores de visitas a páginas, esto no indica que estén menos en el punto de mira de los atacantes. Al contrario, es probable que estos resultados reflejen la concentración de marcas mundiales con grandes bases de clientes en Norteamérica y EMEA, lo que indica un mayor número de posibles víctimas para los adversarios. También podemos atribuir este resultado a la aparición de kits de herramientas de phishing como V3B, que tienen como objetivo específico a los bancos de la Unión Europea desde el año 2023.

Aunque EMEA supera a la mayoría de las regiones en cuanto al número de dominios sospechosos y visitas a páginas, APJ tiene la puntuación promedio de amenazas más alta: 97. América Latina, a pesar de tener el menor número de visitas al sitio, obtiene una sorprendente puntuación promedio de amenaza de 94. Esto indica que los consumidores tanto de Latinoamérica como de la región APJ corren un mayor riesgo de que se les robe su información bancaria y otro tipo de datos confidenciales al visitar sitios web.

Son varios los factores que influyen en el aumento de los peligros del abuso de marca contra los servicios financieros en APJ. En primer lugar, la mayoría de las instituciones de servicios financieros de APJ tienen un nivel muy alto de digitalización: casi todas las ofertas de servicios se pueden realizar online sin necesidad de tener que visitar una sucursal física. La penetración de Internet y la tasa de adopción digital en APJ es una de las más altas del mundo, lo que convierte a esta región en un objetivo atractivo que los ciberdelincuentes pueden aprovechar. En segundo lugar, esta región alberga a algunos de los países donde el uso de redes sociales es más activo de todo el mundo. Además, las instituciones de servicios financieros han intensificado la interacción con los clientes a través de estas plataformas para competir por la cuota de mercado y mejorar los índices de fidelización. El uso generalizado de redes sociales y aplicaciones de mensajería en la región APJ proporciona a los ciberdelincuentes vectores adicionales para distribuir ataques de suplantación de identidad y phishing, a menudo abusando de la confianza que las personas depositan en estas plataformas.



Evolución del cumplimiento: cómo las normativas mundiales sobre ciberseguridad están dando forma a las instituciones financieras

Cuando se le preguntó por qué robaba bancos, el famoso ladrón de bancos Willie Sutton respondió "porque ahí está el dinero". La declaración de Sutton puede aplicarse perfectamente a los ciberataques contra las instituciones financieras actuales. Sin embargo, la motivación de los beneficios financieros solo es una parte de la historia. Las instituciones financieras se encuentran cada vez más en el punto de mira de unos atacantes motivados por cuestiones políticas, así como por aspectos geopolíticos estratégicos. Estas motivaciones, combinadas con el hecho de que "ahí está el dinero", crean una tormenta perfecta para las instituciones financieras, que lideran el grupo como sector industrial con mayor número de ataques.

Esto no debería sorprendernos. El sector financiero siempre ha desempeñado un papel fundamental y central en la sociedad y ha sido objeto de una importante regulación. Aunque la regulación de las instituciones financieras en el pasado se ha centrado en proteger a los consumidores en sus relaciones con ellas, los reguladores actuales intentan aplicar una regulación de seguridad y resiliencia esencial de las infraestructuras a las instituciones financieras y las empresas de servicios. Esta nueva tendencia incluye requisitos no solo para la propia institución financiera, sino también para sus proveedores de tecnologías de la información y la comunicación (TIC).

Existen numerosos ejemplos de normativas de ciberseguridad y resiliencia operativa. En la Unión Europea, la Ley de Resiliencia Operativa Digital (DORA) exige a las entidades financieras y a sus proveedores contar con marcos sólidos de gestión de riesgos de TIC y llevar a cabo pruebas periódicas e informes de incidentes. En Estados Unidos, la Comisión de Bolsa y Valores (SEC) ha introducido normativas sobre la importancia relativa de la ciberseguridad, que exigen a las empresas públicas, incluidas las instituciones financieras, divulgar los incidentes cibernéticos que se produzcan y que pudieran afectar materialmente a sus operaciones. En Australia, la Autoridad Australiana de Reglamentación Cautelar (APRA) ha establecido estándares que exigen que las entidades mantengan capacidades de seguridad de la información acordes con el tamaño y la magnitud de las amenazas a sus activos de información (reglamento CPS 234). En estos ejemplos, se puede notar la tendencia global hacia la mejora de la ciberseguridad y la resiliencia operativa de los sectores financieros para protegerse frente a los riesgos en constante evolución y garantizar la estabilidad financiera.

Teniendo en cuenta estas normativas, las instituciones financieras deben tener la diligencia debida al contratar servicios de TIC y seguridad para asegurarse de que los proveedores cumplan estos estrictos estándares. Deben elegir proveedores que no solo proporcionen un servicio resiliente, sino que también conozcan las normativas pertinentes, proporcionen la visibilidad necesaria para identificar y mitigar las amenazas en evolución, y ayuden a aplicar esa inteligencia a las operaciones en curso.

La visibilidad es fundamental, ya que no puede proteger aquello que no sabe que tiene (o a lo que está conectado) ni tampoco se puede proteger contra una amenaza de la que desconoce su existencia. Servicios como la plataforma Akamai Guardicore no solo ofrecen protección contra ataques, sino que también ayudan a los clientes a entender los flujos de datos, identificar anomalías y segmentar correctamente los activos de red para mitigar las amenazas. Del mismo modo, sus servicios de seguridad de API están diseñados para identificar el tráfico asociado a fin de detectar las API en la sombra, así como para reconocer posibles ataques a través de las API.

Tal vez los bancos deberían añadir visibilidad a la tradicional tríada CIA de la ciberseguridad (confidencialidad, integridad, disponibilidad, por sus iniciales en inglés) para reflejar esta nueva tendencia — VCIA: visibilidad, confidencialidad, integridad y disponibilidad.

James Casey
Vicepresidente y jefe de Privacidad de Akamai

Refuerce sus defensas con Zero Trust

La confianza constituye la base sobre la que las instituciones financieras asientan su reputación. Sin embargo, cuando se trata de proteger entornos complejos y datos confidenciales, la confianza puede convertirse fácilmente en una responsabilidad importante. Los adversarios suelen aprovechar la confianza implícita de muchas maneras, entre las que se incluyen:

- Ataques de phishing para suplantar a individuos dentro de la organización.
- Ataques que aprovechan las vulnerabilidades de seguridad de proveedores externos para acceder a objetivos de gran valor.
- Amenazas internas que acceden ilegalmente con fines nefastos.

La creciente sofisticación de los ataques ha hecho que la seguridad tradicional basada en el perímetro sea inadecuada, ya que considera que todo el tráfico interno es fiable. Teniendo en cuenta el alto riesgo en los servicios financieros, mantener una sólida estrategia de seguridad es fundamental. Aquí es donde el marco Zero Trust se vuelve imprescindible. Este enfoque de seguridad se basa en el principio de que todos los usuarios, los dispositivos y las solicitudes de conexión son potencialmente peligrosos. Implementa la verificación continua y elimina la confianza implícita, denegando el acceso a los recursos de forma predeterminada, a menos que el solicitante esté autenticado y cuente con la autorización necesaria.

Zero Trust mejora el cumplimiento de los requisitos normativos en constante evolución de las instituciones financieras, al proteger los sistemas que gestionan datos regulados, lo que permite a las organizaciones evitar sanciones por auditorías no superadas. Proporciona controles adicionales para los sistemas heredados, lo que ofrece una visibilidad detallada para detectar a los usuarios no autorizados que intentan acceder a aplicaciones esenciales.

El modelo Zero Trust restringe el tráfico este-oeste, al limitar el acceso de red a los sistemas esenciales y evitar el movimiento lateral de amenazas como el ransomware. Esta estrategia de contención protege los datos y activos esenciales al aislar los sistemas infectados. Dado que el número de ataques de ransomware a los servicios financieros ha aumentado considerablemente, no puede subestimarse la importancia de Zero Trust a la hora de proteger la información confidencial. Gracias a su visibilidad detallada, Zero Trust le ayuda a detectar y neutralizar las amenazas en entornos complejos, algo fundamental para evitar la propagación del ransomware y proteger los activos esenciales.

Otra gran ventaja de Zero Trust es su capacidad para proteger los flujos de datos entre aplicaciones, algo esencial para la implementación segura de aplicaciones basadas en la nube. Esto no solo facilita la modernización, sino que también garantiza la protección de la información confidencial en un panorama de amenazas en constante cambio, para permitir a las instituciones financieras innovar sin renunciar a la seguridad. La implementación de un marco Zero Trust mejora la estrategia de seguridad y prepara a una institución para el futuro frente a las amenazas en constante evolución.

La segmentación es buena. La microsegmentación es mejor.

La segmentación es un enfoque arquitectónico que divide una red en segmentos más pequeños con el fin de mejorar el rendimiento y la seguridad. La microsegmentación es una técnica de seguridad que permite dividir lógicamente una red en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual. De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único.

La microsegmentación también es la columna vertebral de Zero Trust. En un informe reciente de Akamai, los responsables de ciberseguridad de los servicios financieros citaron el respaldo a la confianza cero como el factor de impulso más frecuente de la implementación de un proyecto de segmentación. De hecho, casi todos esos responsables que han segmentado están implementando o han implementado ya un marco de seguridad Zero Trust (99 %), aunque menos de la mitad (47 %) afirman que su marco Zero Trust está totalmente definido y completo y, por lo tanto, consolidado.

La microsegmentación funciona con los sistemas existentes y se implementa más rápido que los métodos tradicionales, como los firewalls. Este enfoque permite una respuesta al ransomware más rápida, de hasta 13 horas, y simplifica la gestión en todos los entornos de TI. También ayuda a responder a las necesidades de cumplimiento normativo mediante un control de datos preciso.

Con un ejemplo real se puede ver el efecto de la microsegmentación moderna: en un proyecto se redujo el tiempo de implementación de 2 años a 6 semanas, se utilizó un solo ingeniero y se redujeron los costes en un 85 %. En este caso se muestra cómo la microsegmentación puede ahorrar tiempo y dinero a las organizaciones. Los directores de TI deben comparar estos resultados con los costes de seguridad y el tiempo de implementación actuales.

Para fortalecer su estrategia de ciberseguridad, las instituciones financieras deben priorizar la implementación de estrategias de segmentación avanzadas. Los directores de seguridad de la información deben liderar los esfuerzos por ajustar las medidas de seguridad a los estándares del sector en constante evolución, integrando la microsegmentación como piedra angular de una arquitectura Zero Trust sólida. Los directores de TI deben establecer una cadencia de auditorías de seguridad y actualizaciones de estrategias periódicas para garantizar que sus defensas sean resistentes frente a las sofisticadas ciberamenazas.

Este enfoque proactivo no solo permite mitigar las vulnerabilidades actuales, sino que, al usarlo, las organizaciones también contrarrestan de forma eficaz los desafíos de ciberseguridad emergentes. Al adoptar estas medidas, las instituciones financieras crean un marco de seguridad integral para abordar tanto los problemas inmediatos como la gestión de riesgos a largo plazo.

[La microsegmentación] no solo ayuda a mitigar las vulnerabilidades actuales, sino que también permite a las organizaciones poder hacer frente de forma eficaz a los desafíos de ciberseguridad emergentes.

Mitigación

Cuando se trata de proteger a su institución financiera frente a diversas ciberamenazas, debe implementar un enfoque polifacético. Analicemos las principales estrategias de mitigación para el phishing, la suplantación de marca, los ataques DDoS y el ransomware.

Protección contra el phishing y la suplantación de marca

Para proteger a su institución contra el phishing y la suplantación de marca, plantéese la posibilidad de utilizar servicios de protección de marca de terceros para detectar y eliminar rápidamente el contenido fraudulento. También es importante informar a sus empleados y clientes. Realice actividades periódicas de sensibilización en materia de seguridad para su personal sobre cómo reconocer los intentos de suplantación de identidad y phishing. Proporcione unas directrices claras sobre cómo identificar las comunicaciones legítimas de su institución. Desarrolle un plan de respuesta inmediata para los intentos de suplantación de identidad, incluyendo un procedimiento para informar a los partners y clientes acerca de este tipo de fraudes.

Además, implemente estas técnicas de protección:

- Registre nombres de dominio similares para evitar el typosquatting, y utilice servicios de supervisión de dominios para detectar dominios similares.
- Refuerce los protocolos de autenticación mediante el uso de contraseñas y administradores de contraseñas seguros y únicos, e implemente una autenticación multifactorial (MFA) sólida para todas las cuentas y sistemas.
- Implemente protocolos de autenticación de correo electrónico como Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) y Domain-based Message Authentication, Reporting and Conformance (DMARC) para evitar la suplantación del correo electrónico. Utilice soluciones antiphishing y filtros de correo electrónico avanzados para detectar y bloquear los correos electrónicos maliciosos.
- Proteja su sitio web y sus canales digitales mediante la obtención de certificados SSL, la implementación del protocolo HTTPS y el uso de herramientas antifraude para detectar actividades sospechosas en su sitio web y aplicaciones móviles.
- Proteja los canales de comunicación proporcionando portales seguros e implementando mensajería cifrada para correspondencia confidencial.

Protección contra DDoS

Para proteger a su institución financiera frente a ataques DDoS, se necesita una estrategia de defensa multicapa. Implemente estrategias proactivas, como el uso de productos especializados de detección, mitigación y protección de DDoS, la configuración de la limitación de velocidad y el almacenamiento en caché del contenido en una red de distribución de contenido (CDN). Además, manténgase informado sobre las medidas de seguridad, como la gestión de parches, los planes de respuesta ante incidentes, los controles de mitigación de las direcciones IP expuestas a DDoS y las subredes esenciales, las políticas de control de acceso, la segmentación de la red y los firewalls. Implemente estrategias proactivas, como la configuración de la limitación de velocidad, el almacenamiento en caché del contenido en una CDN y el uso de productos especializados de detección, mitigación y protección contra DDoS.

Para proteger la infraestructura de DNS, supervise y analice de forma constante el tráfico de DNS entrante y opte por una plataforma híbrida en lugar de un firewall de DNS tradicional. Entender las tácticas, las técnicas y los procedimientos que utilizan los atacantes le ayudará a protegerse mejor contra los ataques DDoS.

Protección contra ransomware

Como se ha mencionado anteriormente en este informe, lograr la confianza cero (Zero Trust) con la segmentación de la red, especialmente la microsegmentación, resulta fundamental para limitar la propagación del ransomware en toda su institución financiera. La implementación de medidas sólidas de ciberseguridad como esta ayudará a combatir las técnicas avanzadas que están empleando los autores de este tipo de ataques. Además, esté alerta y utilice el marco de MITRE ATT&CK para obtener información sobre las tácticas y técnicas más frecuentes utilizadas por los atacantes y reforzar sus guías en consecuencia para acabar con la cadena de exterminio del ransomware.

Actualice continuamente sus defensas e informe a su personal para que reconozca y responda eficazmente a las posibles amenazas. Incorpore sólidas defensas perimetrales, protección de terminales, filtrado de correo electrónico y la gestión habitual de parches. Implante una supervisión continua del tráfico de red, los registros del sistema y el comportamiento de los usuarios, e implemente prácticas de detección de amenazas para identificar de forma proactiva las amenazas de ransomware.

Cree periódicamente copias de seguridad de los datos, incluidas copias aisladas, para garantizar que la información esencial se pueda restaurar rápidamente en caso de un ataque de ransomware. Implemente la autenticación multifactorial (MFA) en todas las cuentas de usuario para añadir una capa adicional de seguridad.

Con estas estrategias de mitigación completas puede aumentar significativamente la capacidad de su institución financiera de defenderse ante diversas ciberamenazas, garantizar la continuidad operativa, proteger su reputación y mantener la confianza de los clientes.

Conclusión

A medida que su institución financiera adopte la transformación digital para mejorar la experiencia del cliente, la eficiencia operativa y el posicionamiento ante la competencia, los desafíos de seguridad se intensificarán, junto con la creciente presión para gestionar un panorama normativo en constante evolución. En esta edición del informe SOTI, hemos analizado las amenazas persistentes y emergentes a las que se enfrenta el sector de los servicios financieros, subrayando la necesidad de una evaluación y mejora continuas de las soluciones de seguridad. A medida que las amenazas se vuelven más sofisticadas, resulta fundamental ir un paso por delante fortificando las defensas y perfeccionando las estrategias de seguridad.

Ahora que los ataques DDoS a las instituciones financieras superan a los del sector de los videojuegos, considerado desde hace mucho como el principal objetivo, esta alarmante tendencia pone de relieve el aumento de los riesgos. Factores como el hacktivismo y el clima geopolítico han hecho que los servicios financieros sean más vulnerables que nunca. Al mismo tiempo, destacan la magnitud y la gravedad del tráfico generado por los sitios de suplantación de marca y de phishing que tienen como objetivo a las instituciones financieras, junto con la velocidad a la que los atacantes pueden generar nuevos dominios después de que se hayan desmantelado los sitios iniciales. Para el seguimiento de estas actividades las organizaciones pueden necesitar muchos recursos, y los equipos de seguridad necesitan soluciones que incluyan servicios de neutralización, inteligencia contra amenazas y detección de suplantación de marca y phishing en varios canales digitales.

Los consumidores y los reguladores suelen responsabilizar a las instituciones financieras, incluso cuando estas no son directamente culpables, después de ser víctimas de phishing y de otro tipo de estafas. Más importante aún, el phishing y la suplantación de marcas a menudo sirven como precursores de ataques más peligrosos, lo que hace que sea esencial cortar el ciclo de ataque desde las fases iniciales. Tomar medidas decisivas puede significar la diferencia entre convertirse en el titular de mañana debido a una filtración y proteger la reputación de su institución y la confianza de los clientes.

Dada la naturaleza incesante de los ataques contra las instituciones financieras, salvaguardar la información confidencial para prevenir el fraude y el abuso sigue constituyendo un gran reto. La adopción de un marco de seguridad como Zero Trust es esencial para defenderse eficazmente contra los ataques de phishing dirigidos a los empleados, así como para evitar que el ransomware se extienda por las redes para llegar a los activos críticos, todo ello a la vez que se garantiza el cumplimiento de las normativas globales existentes y emergentes.

Este informe proporciona información útil sobre las últimas tendencias de ataque en el sector de los servicios financieros, lo que le permite reforzar sus defensas. Si se mantiene alerta e implementa las estrategias descritas en este informe, podrá proteger mejor a su organización y a sus clientes ante un panorama de amenazas que no deja de crecer.

Manténgase informado sobre nuestra investigación más reciente visitando nuestro Centro de investigación sobre seguridad.

Metodología

DDoS (capa 7)

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 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.

DDoS (capas 3 y 4)

Akamai Prolexic Routed defiende a las organizaciones de los ataques DDoS y otro tipo de tráfico no deseado o malicioso deteniéndolos antes de que lleguen a las aplicaciones, los centros de datos y las infraestructuras de Internet en la nube o híbridas (públicas o privadas), incluidos todos los puertos y protocolos. Los expertos del centro de control de operaciones de seguridad (SOCC) de Akamai pueden adaptar los controles de mitigación proactivos para detectar y detener los ataques al instante, y realizan análisis en tiempo real del tráfico restante para implementar medidas de mitigación adicionales si es necesario. Estos ataques mitigados se organizan y agrupan en eventos de ataques, y el SOCC registra todos los datos asociados para analizarlos.

Los datos de este informe cubren el periodo de 18 meses que abarca desde el 1 de enero de 2023 hasta el 30 de junio de 2024, a menos que se indique lo contrario.

Ataques de suplantación de marca

Akamai Brand Protector es una solución antiabuso diseñada para proteger a las empresas y a sus clientes frente a ataques de suplantación de marca, como phishing, sitios web falsificados, cuentas falsas en redes sociales y aplicaciones no autorizadas. La solución utiliza la red mundial de Akamai, donde se analizan más de 900 TB de datos diariamente, para detectar amenazas antes de que afecten a los clientes. Esta inteligencia se complementa con fuentes externas de partners para ofrecer una amplia visión de las posibles amenazas en las distintas plataformas online.

Se analizan diversas características de cada uno de los dominios sospechosos detectados y sus niveles determinados de riesgo influyen en la puntuación de amenaza calculada del dominio. Estos dominios sospechosos se supervisan, se realiza un seguimiento de los datos asociados y se avisa a los clientes afectados de estas campañas maliciosas que intentan suplantar la identidad de la marca.

Los datos de este informe analizan dominios sospechosos detectados en el periodo de 12 meses que abarca desde el 1 de agosto de 2023 hasta el 31 de julio de 2024.

Créditos

Director de investigación

Mitch Mayne

Editorial y redacción

James Casey
Badette Tribbey
Lance Rhodes

Revisión y expertos en la materia

Cheryl Chiodi
Gal Meiri
Ziv Eli
Richard Meeus
Reuben Koh
Steve Winterfeld

Análisis de datos

Chelsea Tuttle

Materiales promocionales

Barney Beal

Marketing y publicación

Georgina Morales
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 a los servicios financieros, visite nuestra **página de servicios financieros**.