WHITE PAPER

La rápida evolución y la creciente amenaza de los ataques DDoS

Los ataques cada vez son más selectivos, sofisticados y frecuentes, por lo que las empresas deben permanecer alerta.

Ninguna empresa escapa ya a los ataques distribuidos de denegación de servicio (DDoS). Los ciberdelincuentes, que utilizan tácticas como la extorsión, el hacktivismo o la venganza, pueden atacar con facilidad a cualquier empresa con ataques sofisticados y de gran tamaño. Por este motivo, todas las empresas orientadas a los medios digitales necesitan una defensa integral contra ataques DDoS en la actualidad.

Uno de los primeros tipos de ataques de Internet

El 22 de julio de 1999, 114 ordenadores infectados saturaron un único ordenador de la Universidad de Minnesota con paquetes de datos superfluos y lo dejaron sin servicio durante dos días.

Según MIT Technology Review, este fue el primer ataque DDoS documentado.

En las semanas y meses siguientes, otras grandes empresas, como la CNN o Amazon, sufrieron pérdidas de conexión, a medida que los hacktivistas y otros ciberdelincuentes se daban cuenta de lo fácil que era lanzar esos ataques. Todo lo que necesitaban eran unas pocas líneas de código.

Los ataques DDoS se convirtieron en una amenaza para cualquier empresa con presencia online.

Los ataques crecen en tamaño y complejidad

La defensa frente a ataques DDoS ha llegado muy lejos desde 1999. Sin embargo, los delincuentes también han evolucionado. Los agentes de amenazas DDoS actuales cuentan con docenas de vectores de ataque que pueden aprovechar y kits de herramientas de ataque de bajo coste. Asimismo, disponen de innumerables dispositivos vulnerables en Internet que les permiten amplificar sus campañas. En 2016, los atacantes dejaron sin conexión a una gran parte de Internet utilizando grabadoras de vídeo digital (DVR) de cámaras de seguridad infectadas.

Desde entonces, cientos de millones de dispositivos del Internet de las cosas (IoT) se han conectado a la red sin protección. La próxima revolución del 5G anticipa que el número de estos dispositivos seguirá creciendo. Imagine la potencia y el tamaño de los ataques impulsados por las mejoras exponenciales del 5G en términos de velocidad, capacidad y latencia.

También crece a pasos agigantados el número de servidores desprotegidos y sin mantenimiento en Internet que los delincuentes pueden secuestrar para llevar a cabo ataques de amplificación y reflexión. Muchos de estos servidores (cuyas direcciones IP conocen los delincuentes) pueden multiplicar las solicitudes falsificadas por más de 50 000.

Mitigación y protección de emergencia ininterrumpidas frente a ataques DDoS

Los clientes actuales de Akamai que han sido amenazados con un ataque DDoS deben ponerse en contacto con el Centro de control de operaciones de seguridad (SOCC) de Akamai.

Si no es cliente de Akamai, pero necesita protección de emergencia, rellene el formulario en nuestra **página de línea directa de información sobre DDoS**, o llame al **+1-877-425-2624** para obtener asistencia inmediata.

Ningún sector es inmune a los ataques DDoS

Actualmente, Akamai mitiga miles de ataques DDoS cada año.

En algunos casos, los motivos parecen obvios. Un jugador puede utilizar ataques DDoS para ralentizar las redes y obtener una ventaja competitiva frente a los jugadores rivales. En otra ocasión, unos estudiantes universitarios utilizaron ataques DDoS dirigidos para frustrar a los clientes de un proveedor de servicios de Internet (ISP) y mejorar el negocio de la competencia.

No obstante, a veces los motivos son más complejos o esquivos. Hemos sido testigos de cómo los delincuentes utilizan ataques DDoS para distraer a los equipos de respuesta ante incidentes en un área de una organización, al tiempo que dirigen otro ataque menos obvio en otra parte.

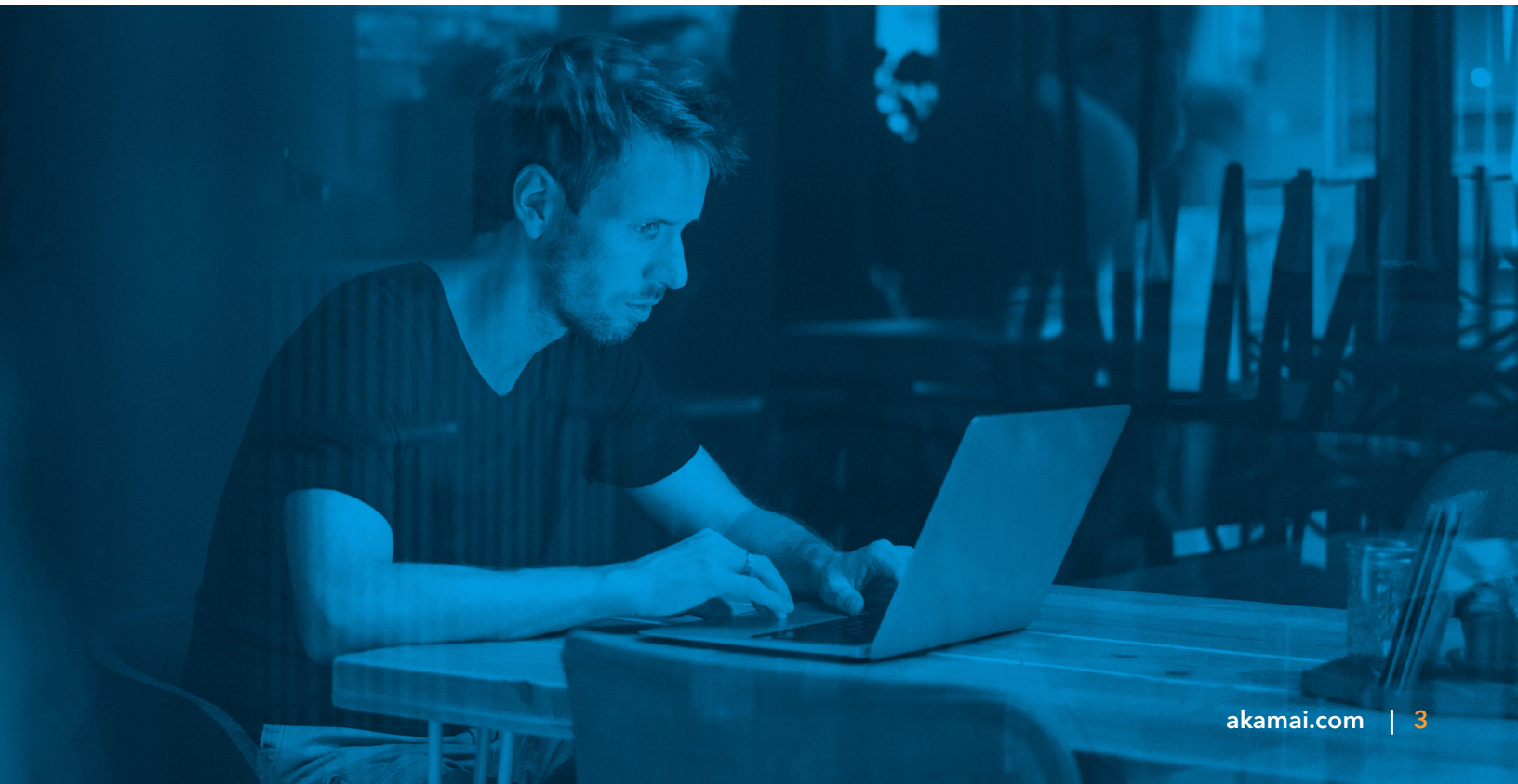
Para los agentes maliciosos que no tienen los conocimientos necesarios, existen empresas de "ataques DDoS de alquiler" que ofrecen sus servicios en la Darknet. Los precios van desde los 5 USD por un ataque de 5 minutos hasta los 400 USD por uno de 24 horas. Si alguien tiene alguna cuenta pendiente, puede gastarse 200 o 300 USD y generarle pérdidas millonarias a una empresa.

2020 trajo consigo ataques de mayor tamaño y más complejos

Durante la primera mitad de 2020, Akamai detuvo ataques masivos de 1,44 terabits por segundo (Tbps) y 809 millones de paquetes por segundo (Mpps), el mayor ataque Mpps registrado.

Aunque se mitigaron en menos de un segundo, estos ataques reflejan una tendencia hacia más ataques de 100 Gbps o incluso de mayor tamaño. Muchos utilizan combinaciones únicas y complejas de varios vectores. Su objetivo es saturar o eludir las defensas y consumir los recursos de respuesta ante incidentes.

Los ataques que requieren un mínimo de mitigación humana, no solo respuestas automatizadas, también van en aumento.



La campaña de extorsión DDoS más grande de la historia

En agosto de 2020, el equipo de investigación de inteligencia de seguridad de Akamai emitió una alerta, en la que se advertía que empresas de diferentes sectores habían recibido correos electrónicos de extorsión DDoS. Los atacantes amenazaron con paralizar las operaciones e insinuaron que las empresas se enfrentarían a un tiempo prolongado de inactividad y grandes pérdidas financieras si no pagaban un rescate en bitcoin.

Solo unas semanas después, el FBI informó de que miles de empresas de todo el mundo habían recibido correos electrónicos de extorsión similares. Los atacantes irrumpían y amenazaban a las empresas de un sector y, a continuación, volvían a hacer lo mismo en otro y así sucesivamente. Los atacantes más organizados suelen volver a amenazar a los objetivos anteriores.

Cuanto mejores sean sus defensas, menos probabilidades tendrá de ser atacado

Los ciberdelincuentes se comportan como cualquier otro delincuente. "Fichan" y buscan una debilidad. En el caso de los ataques DDoS, eso significa buscar en el sistema de nombres de dominio (DNS), las aplicaciones web y los activos de los centros de datos orientados a Internet de sus víctimas potenciales.

Si en este reconocimiento detectan recursos, sitios o servicios vulnerables, los ciberdelincuentes puede intentar dirigir un ataque, mientras que si descubren defensas reforzadas no suelen intentarlo.

De hecho, entre los nuevos clientes del servicio de emergencia de Prolexic que habían sido atacados antes de adoptar la plataforma, la gran mayoría no han vuelto a recibir ataques después de implementar las defensas de Prolexic. Los objetivos defendidos por Prolexic no suelen merecer la pena para los ciberdelincuentes, sobre todo cuando hay más posibilidades en otros lugares.

Funcionamiento de una defensa holística contra ataques DDoS

Akamai proporciona protección exhaustiva frente a ataques DDoS mediante una red transparente de soluciones específicas de mitigación de barrido en la nube, de DNS distribuido y en el borde de Internet con más de 175 Tbps de capacidad total de la red. Estas nubes están especialmente diseñadas para fortalecer las estrategias de seguridad frente a DDoS, al tiempo que reducen las superficies de ataque. Esta protección integral contra DDoS está diseñada para mejorar la calidad de la mitigación y reducir los falsos positivos, así como para aumentar la resiliencia frente a los ataques más grandes y complejos.

Además, la solución se puede adaptar a los requisitos específicos de las aplicaciones web y los servicios online.

Protección en el borde de Internet

Akamai diseñó Intelligent Edge Platform, una plataforma distribuida a nivel mundial, como un proxy inverso que solo acepta tráfico a través de los puertos 80 y 443. Todos los ataques DDoS en la capa de red se contrarrestan en el borde de Internet con un acuerdo de nivel de servicio (SLA) que garantiza una resolución inmediata.

En el caso de los eventos en la capa de aplicación, incluidos los que se lanzan a través de API, Kona Site Defender absorbe los ataques, a la vez que permite acceder a los usuarios legítimos.

Protección de DNS

El servicio DNS autoritativo de Akamai, Edge DNS, también filtra el tráfico en el borde de Internet. A diferencia de otras soluciones de DNS, Akamai ha diseñado Edge DNS específicamente para ofrecer disponibilidad y resiliencia frente a ataques DDoS. Edge DNS también ofrece un rendimiento superior con redundancias de arquitectura en varios niveles, incluidos servidores de nombres, puntos de presencia, redes e incluso nubes de IP Anycast segmentadas.

Protección de barrido en la nube

Prolexic protege centros de datos enteros e infraestructuras híbridas contra ataques DDoS, en todos los puertos y protocolos, con 20 centros de barrido globales y 8,2 Tbps de defensa específica contra DDoS. Esta función está diseñada para mantener los recursos online disponibles, un pilar fundamental de cualquier programa de seguridad de la información.

Como servicio totalmente gestionado, Prolexic permite diseñar modelos de seguridad positivos y negativos. El servicio combina defensas automatizadas con mitigación por parte de los expertos de la red global del SOCC de Akamai. Prolexic también ofrece un SLA de mitigación de cero segundos **líder en el sector** a través de controles defensivos proactivos.

Cómo detuvo Prolexic un ataque récord

El ataque de 809 Mpps de junio de 2020 fue el ataque de paquetes por segundo (PPS) más grande jamás visto en Internet. A diferencia de los ataques de bits por segundo más comunes, que intentan saturar el canal de entrada de Internet, los ataques PPS se establecen para agotar el equipo de red en el centro de datos o la nube.

Este formidable ataque implicó una gran cantidad de direcciones IP de origen. Más del 96 % de estas direcciones no se habían observado anteriormente en otros ataques. El ataque también creció de 418 Gbps a 809 Mpps en solo dos minutos.

Afortunadamente, la empresa objetivo era un cliente de Prolexic y contaba con un SLA de cero segundos. El SOCC de Akamai trabajó con este cliente para comprender sus perfiles de referencia de tráfico en tiempos de paz y establecer controles y políticas de seguridad para bloquear ataques DDoS al instante.

Programe una sesión informativa personalizada sobre amenazas hoy mismo

Visite **akamai.com/ddos-briefing**