SOTI VERANO 2018

[Estado de Internet] / Seguridad

RESUMEN EJECUTIVO

Resumen ejecutivo

Akamai, el principal y más respetado proveedor de servicios de distribución de contenido en la nube de todo el mundo, utiliza su plataforma, conocida como Akamai Intelligent Platform™ y distribuida globalmente, para procesar billones de transacciones al día en Internet. Esto nos permite recopilar enormes cantidades de datos sobre diversos parámetros relativos a la conectividad de banda ancha, la seguridad en la nube y la distribución de contenido multimedia. Cada trimestre, Akamai publica informes sobre el estado de Internet elaborados a partir de estos datos, en los que se abordan aspectos relacionados con la conectividad de banda ancha y la seguridad en la nube.

IMPLICACIONES PARA LA EMPRESA

Los ataques de los que hemos sido testigos los últimos meses nos recuerdan que el estado de Internet, en materia de seguridad, no es algo invariable. El ingenio de los atacantes nunca descansa. Siguen descubriendo nuevos vectores, explotando nuevas vulnerabilidades y desarrollando estrategias de ataque mucho más dañinas que sus predecesoras. En 2017, vimos cómo se utilizaron nuevas clases de dispositivos, tales como teléfonos móviles y dispositivos de IoT, para formar enormes botnets con las que se perpetuaron ataques que batieron récords. Sin embargo, en los dos primeros meses de 2018, todos estos récords volvieron a superarse: los atacantes hallaron en Memcached, un servicio que ni siquiera estaba destinado a exponerse en Internet, un nuevo vector para generar ataques que alcanzaron la ingente cifra de 1 Tbps. Memcached permite que los ataques se amplifiquen con solicitudes de una magnitud mucho mayor que cualquier otro ataque de reflexión conocido.

Afortunadamente, en este caso, una respuesta rápida por parte de desarrolladores, operadores de redes y proveedores de servicios parece haber reducido en poco tiempo el número de servidores de Memcached vulnerables disponibles, por lo que se espera que el potencial de este nuevo vector de ataque se vea limitado en el futuro. Pero es un recordatorio contundente de que la comunidad de seguridad nunca puede bajar la guardia; debemos conocer las tendencias de ataque y los avances tecnológicos, y estar preparados para ataques de cada vez mayor tamaño. Asimismo, todos los miembros de la comunidad tienen la responsabilidad de instalar los últimos parches de software y establecer configuraciones seguras para minimizar el acceso de los delincuentes a las superficies de ataque.

RESUMEN DE LOS EDITORES

El estado de Internet en cuanto a seguridad está en constante evolución; nuestro informe no iba a ser menos. Estamos implementando cambios en la frecuencia de publicación, el formato y la estructura, con el objetivo de ofrecer a los lectores información sobre nuestros datos e investigaciones de la manera más oportuna y relevante posible. Por ejemplo, gran parte de los datos estadísticos y los gráficos relacionados con los ataques de DDoS y a aplicaciones web (incluidos gráficos sobre el tamaño y la frecuencia vectorial de ataques DDoS) se ha trasladado a nuestro sitio web. Puede consultarse la información más reciente al respecto en nuestro blog. Además, empezaremos a publicar con regularidad informes más resumidos que se centren en las tendencias a largo plazo, la investigación y el análisis. El informe *Estado de Internet en materia de seguridad: Ataques web* tendrá carácter bianual, con la publicación de un número en invierno y otro en verano.

Nuestra sección "Información sobre ataques" del verano de 2018 se centra en el ataque reflector de Memcached perpetrado en el pasado mes de febrero, que se convirtió en el nuevo mayor ataque mitigado por Akamai hasta la fecha. Al llegar a los

1 Tbps

Umbral superado por el reflector Memcached

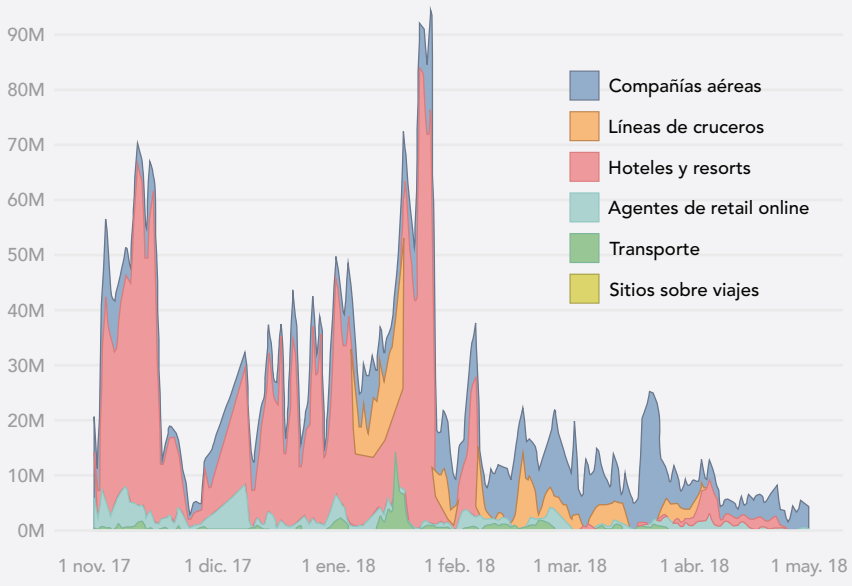
1,3 Tbps, el ataque superó el doble el récord anterior de 623 Gbps, alcanzado por Mirai en septiembre de 2016. También siguió aumentando a lo largo del año pasado el tamaño medio de los ataques DDoS, ahora establecido en 1,3 Gbps, lo que demuestra la importancia que tiene para toda organización estar preparada para actuar ante ataques a gran escala.

En el informe *Estado de Internet en materia de seguridad del verano de 2018: Ataques web*, examinamos algunos ataques DDoS que recurren a tácticas inusuales para incrementar su efectividad. Si bien la mayoría de los ataques DDoS son simples y volumétricos, en algunos se aprecia la influencia de enemigos inteligentes y adaptables que cambian de táctica para eludir los sistemas de defensa.

Destaca la iniciativa Operation Power Off, una actuación policial para cerrar los sitios web de DDoS de alquiler. Las fuerzas policiales de varios países colaboraron en abril de 2018 para cerrar el sitio web Webstressser.org, uno de los más conocidos en el mercado de DDoS de alquiler, presuntamente responsable de millones de ataques. Sabiendo lo lucrativos que son estos sitios, es probable que surjan otros para ocupar su lugar.

Por último, siguiendo con el análisis de los datos de abuso de credenciales y bots que presentamos en el informe *Estado de Internet en materia de seguridad del cuarto trimestre de 2017*, profundizamos en la cuestión para elaborar un perfil de los bots y los abusadores de credenciales que atacan el sector de la hostelería, que fue el que sufrió, con diferencia, el mayor porcentaje de intentos maliciosos de inicio de sesión. También observamos que el cierre de varias rutas a principios de febrero de 2018 parece haber precipitado una considerable disminución del tráfico malicioso.

Fig. 1.1 **Intentos maliciosos de inicio de sesión: sector hotelero y de viajes**



ATAQUES DDOS: VERANO 2018 VS. VERANO 2017

16 % de aumento en el número total de ataques DDoS

16 % de aumento en los ataques a la capa de infraestructura (capas 3 y 4)

4 % de aumento en los ataques basados en reflexión

38 % de aumento en los ataques a la capa de aplicación

Para consultar otros análisis e investigaciones, descargue el informe completo.

El informe *Estado de Internet en materia de seguridad del verano de 2018: Ataques web* incluye datos sobre ataques extraídos de la infraestructura global de Akamai e investigaciones de diversos equipos de la organización.

ESTADO DE INTERNET. EQUIPO DE SEGURIDAD

Jose Arteaga, Akamai SIRT, gestor de datos — Información sobre ataques
Dave Lewis, especialista en seguridad global — Operation Power Off
Wilber Mejia, Akamai SIRT — Información sobre ataques
Elad Shuster, analista de seguridad de datos de DDoS avanzado — Blog de Akamai
David McEwan, Centro de Control de Operaciones de Seguridad — DDoS avanzado
Alejandro Ziegenhirt, Centro de Control de Operaciones de Seguridad — DDoS avanzado

PERSONAL EDITORIAL

Martin McKeay, experto principal en seguridad, editor sénior
Amanda Fakhreddine, redactora técnica sénior, editora

EQUIPO CREATIVO

Shawn Broderick y Sajeesh Alakkaparambil, diseño
Georgina Morales Hampe y Kylee McRae, gestión de proyectos

ACERCA DE AKAMAI

Akamai, la plataforma de distribución en la nube más grande y respetada del mundo, ayuda a sus clientes a ofrecer las mejores y más seguras experiencias digitales, independientemente del dispositivo, en cualquier momento y en cualquier lugar. La plataforma ampliamente distribuida de Akamai ofrece una escala inigualable, con más de 200 000 servidores repartidos por 130 países, para garantizar a sus clientes el máximo rendimiento y protección frente a las amenazas. La cartera de soluciones de rendimiento web y móvil, seguridad en la nube, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente excepcional y una supervisión ininterrumpida. Para descubrir por qué las principales instituciones financieras, líderes de retail online, proveedores de contenidos multimedia y de entretenimiento, y organizaciones gubernamentales confían en Akamai, visite www.akamai.com/es/es, blogs.akamai.com/es/, o siga a @Akamai en Twitter. Encontrará nuestra información de contacto global en www.akamai.com/locations; también puede llamar al +34 91 793 32 43. Publicado en junio de 2018.