[Estado de Internet] / Seguridad

RESUMEN ANUAL

RESUMEN EJECUTIVO: VOLUMEN 4, NÚMERO 5

NOTAS DEL EDITOR

Desde noviembre de 2017, el equipo de investigación de Akamai ha publicado, de media, al menos un artículo, entrada de blog o documento a la semana. Estas publicaciones abarcan entradas sobre próximos eventos, comunicaciones de crisis sobre amenazas emergentes y el propio informe sobre el estado de Internet en materia de seguridad. Esta es la razón por la que hemos decidido echar la vista atrás para valorar nuestro trabajo en seguridad y ver cómo se sitúa en un recorrido más amplio al incluir también el panorama del año pasado. Con esto presente, hemos pedido a Andy Ellis, director jefe de Seguridad, que nos ofrezca su opinión sobre dónde nos pueden llevar las tendencias actuales en 2019. La información que se presenta a continuación es un extracto de su ensayo.

OFICINA DEL CSO

“ plus ça change, plus c’est la même chose —
Jean-Baptiste Alphonse Karr

Si algo es cierto sobre las tendencias del sector de la seguridad en Internet, es que la historia se repite año tras año. En 1998, durante la operación Zorro del desierto, los adversarios utilizaron un ataque distribuido de denegación de servicio, que además se aprovechó de la vulnerabilidad de *lágrima*, para tratar de bloquear las redes de USCENTAF. Por entonces, yo era el ingeniero de defensa encargado de la misión, por lo que recuerdo la emoción de identificar el ataque, probar una configuración y finalmente llevarlo a nuestros sistemas de seguridad perimetral. Esta historia no difiere estratégicamente de las acciones que tienen lugar en nuestros propios centros de operaciones de seguridad y en los de terceros cada día; solo han cambiado la escala y la automatización.

Por lo tanto, de cara al 2019, es más sencillo detectar los patrones recurrentes de los últimos años, sugerir que van a continuar y suponer que probablemente evolucionen en su gran mayoría de la forma en la que venían haciéndolo.

Akamai
Experience the Edge

DDoS DE FUERZA BRUTA

DDoS es siempre un buen punto de partida, ya que las tendencias en este tipo de ataques son notablemente estables. La forma más sencilla de concebir los ataques es abordarlos partiendo de dos ejes diferenciados: el aprovechamiento y el ancho de banda. El *ancho de banda* es simplemente la medición del tráfico que un adversario puede generar en un momento dado. En el pasado, hemos observado cómo el tamaño del mayor ataque aumentaba en torno a un 9 % por trimestre, lo que significaría que llega a duplicarse cada dos años. Pero sorprendentemente no se trata de un crecimiento continuo, ya que se alcanzan nuevos picos (junto a la curva intertrimestral del 9 %) cada vez que un adversario descubre una nueva forma de construir una botnet o una reflexión, como fue el caso de los ataques de reflexión de Memcached o Mirai.

En el periodo entre los nuevos picos, suceden dos cosas. En primer lugar, las partes afectadas, como los administradores de sistemas y los operadores de proveedores de servicios de Internet (ISP), toman medidas para reducir el número de sistemas disponibles para el uso durante los ataques. En segundo lugar, los adversarios comienzan a luchar por tomar el control de estos recursos, y se puede observar cómo las botnets empiezan a fragmentarse, lo que resulta en ataques individuales de menor tamaño.

Desde el punto de vista de la eficacia, esto no tiene por qué perjudicar al atacante. Por lo general, el tamaño de los estilos de defensa DDoS no se amplía de manera lineal. Los ataques más grandes suceden en el perímetro de la red, lugar donde se sitúan servicios como Kona Site Defender y Prolexic Routed de Akamai. Las defensas de nivel medio se establecen en el núcleo de los ISP y proporcionan servicios de "conexión limpia" a los propietarios del sitio. Por último, las defensas de menor tamaño, las soluciones locales, se instalan solo en los centros de datos de destino. Un adversario cuya botnet no es lo suficiente grande como para dirigirla a una defensa basada en el perímetro, puede realizar un ataque a defensas basadas solo en el centro de datos y ser efectivo incluso aunque tenga un tamaño cien veces menor.

Dado que los ataques DDoS basados en el ancho de banda adoptan formas muy diversas, llama la atención que el tamaño máximo de los ataques siempre parezca limitarse a una curva de crecimiento trimestral del 9 %. Un dato curioso que tiene explicación. Esta tendencia no se debe a una especie de límite natural. La explicación más probable es que sea el crecimiento de Internet subyacente el que limita la capacidad de adición de las botnets. La capacidad de Internet atenúa el peso total de lanzamiento que un ataque DDoS puede generar: cuanto mayor sea la distancia entre el objetivo y los componentes de una red, menor será el tráfico que logrará traspasar cualquier enlace congestionado entre el objetivo y el origen del ataque.

Si quiere obtener más información sobre la opinión de Andy en relación con DDoS, los ataques a la capa de aplicación, el relleno de credenciales, la denominada gig economy y las cadenas de bloques, descargue el informe **Estado de Internet en materia de seguridad: resumen anual**, volumen 4, número 5.

ACERCA DE AKAMAI

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma perimetral inteligente de Akamai llega a todas partes, desde la empresa a la nube, lo que permite a nuestros clientes y a sus negocios ser rápidos, inteligentes y seguros. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas a raya. La cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente excepcional, análisis y una supervisión ininterrumpida durante todo el año. Para descubrir por qué las marcas más importantes del mundo 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 diciembre de 2018.