LA **BOTNET MIRAI**, RESPONSABLE DE LOS ATAQUES MÁS POTENTES Y **DEVASTADORES**

La intensidad de los ataques DDoS ha aumentado notablemente, duplicando su tamaño durante el año 2016. Se trata de ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés) más complejos y devastadores, cuya contención exige conocimientos más especializados que en el pasado. No se restringen, además, a ningún sector concreto.

El 21 de octubre de 2016, una serie de ataques DDoS a través de Internet de las cosas contra la infraestructura de DNS gestionada por Dyn impidió el acceso de los usuarios a los sitios web más importantes de EE. UU., entre otros, Twitter, Spotify o PayPal. Dyn no es cliente de Akamai, por lo que no participamos en la mitigación de ese ataque. Sin embargo, un mes antes, Akamai había mitigado un enorme ataque DDoS de 623 Gbps, en el cual estaba involucrado el mismo malware causante de la infección: la botnet Mirai. El ataque de 623 Gbps fue solo uno de los diez ataques basados en Mirai que apuntaron a un mismo objetivo durante un periodo de ocho días, cinco de los cuales alcanzaron un pico superior a 100 Gbps.

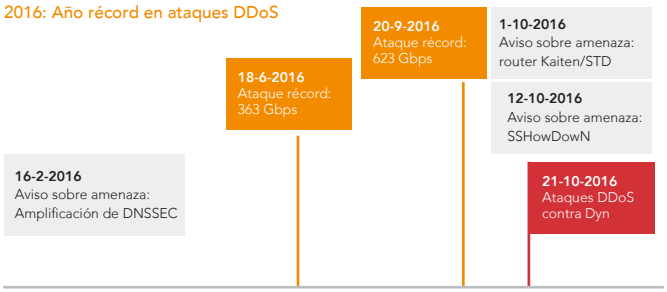
El ataque contra Dyn demuestra que, aparte de los ataques directos, las organizaciones también deben gestionar el riesgo de sufrir ataques DDoS contra la infraestructura central de Internet, por ejemplo, los servidores DNS. Un ataque contra dicho objetivo puede tener un efecto dominó en cualquier organización que, directa o indirectamente, confíe su presencia en Internet a un proveedor vulnerable.

Botnet Mirai y el Internet de las cosas

El malware Mirai se aprovecha de centenares de miles de dispositivos inteligentes conectados. Instala el malware, se hace con el control y recluta un ejército mundial obteniendo acceso a dispositivos con contraseñas predeterminadas faltas de seguridad. A continuación, cada uno de los dispositivos infectados explora Internet con el propósito de identificar e infectar otros dispositivos vulnerables, mientras espera la requisición para el ataque DDoS.

El Internet de las cosas cosas (IoT, por sus siglas en inglés) consta de miles de millones de dispositivos con capacidad para enviar y recibir datos, que se hallan en domicilios particulares, oficinas y la sociedad en general. Los dispositivos de IoT que infecta el malware Mirai son los equipos de seguridad domiciliaria y los equipos de entretenimiento, como cámaras web, grabadoras de vídeo digital o routers.

Un agente malicioso filtró al público en general el código fuente de Mirai, junto con instrucciones para crear una botnet. A las dos semanas de la publicación del código, Akamai observó la primera tanda de capacidades actualizadas. La laxitud de la seguridad y la vulnerabilidad del firmware en millones de dispositivos de IoT los convierte en carne de cañón para los ataques DDoS. La botnet Mirai tiene visos de seguir creciendo, tanto en número como en fuerza.



Ataques DDoS a proveedores de servicios de DNS

En un informe de Forrester elaborado tras los ataques a Dyn, los investigadores constatan lo siguiente: "Muchas de las empresas afectadas por el ataque vieron imposibilitada la recuperación porque habían introducido un punto único de fallo en sus servicios y dependían de un solo proveedor de DNS autoritativo principal, pero carecían de uno secundario".[1]

Los ataques a Dyn no tenían a Akamai como objetivo, ni afectaron a sus servicios. Akamai conserva un historial de direcciones IP, la última de las cuales se utiliza en caso de que quede inactivo el sistema DNS. Eso permitió a Akamai resolver casi 60 000 solicitudes de DNS por segundo que, de otro modo, no se hubiesen resuelto, y mantener online a los clientes que usaban el sistema DNS gestionado por Dyn.

Por qué Akamai: diseño perfecto para resistir los ataques DDoS

Los servicios de Akamai están concebidos para resistir los ataques DDoS. Akamai protege a sus clientes contra los ataques DDoS con Akamai Intelligent Platform™, la red Prolexic y la infraestructura distribuida Fast DNS. No dejamos de invertir en mejorar la resistencia a los ataques DDoS de esas plataformas como prevención ante actuaciones de los adversarios.

> Las empresas han de reforzar más la resistencia cuanto más baja es la barrera de entrada de la interrupción y la degradación de la actividad digital.[2]

En el ámbito general, nuestro modelo de planificación de la capacidad parte de los mayores ataques DDoS que hayamos verificado y multiplica ese tráfico por un factor de escala con el fin de ofrecer un amplio margen en caso de que los ataques aumenten de tamaño. El resultado es que hemos logrado mitigar los mayores y más sofisticados ataques DDoS de la historia, incluidos los ataques de Qassam Cyber Fighters a entidades financieras estadounidenses y, en septiembre, el ataque récord, cifrado en 623 Gbps, a un cliente de Akamai al que no se le cobraba el servicio.

Nuestro equipo de Adversarial Resilience evalúa de forma constante las nuevas amenazas e incidentes para detectar posibles puntos débiles en los sistemas de Akamai y colabora con los equipos de ingeniería con el fin de mejorar la resistencia.

Resistencia a ataques DDoS en Akamai Intelligent Platform

Akamai mantiene una capacidad global suficiente para absorber los ataques DDoS de mayor tamaño. Aparte de la capacidad, diseñamos nuestra red de distribución de contenido (CDN, por sus siglas en inglés) de modo que ofrezca disponibilidad y resistencia en cualesquier condición adversa, no solo en caso de un ataque DDoS.

La CDN de Akamai conecta a los usuarios finales con el servidor perimetral de Akamai óptimo, según sea el estado de cada servidor, y desvía el tráfico de los usuarios de forma automática para circunvalar las interrupciones de la red local.

Con más de 220 000 servidores en activo actualmente en todo el mundo, Akamai puede mantener la conectividad en las condiciones más adversas, desde la congestión de la red hasta los ataques DDoS, pasando por las interrupciones de los proveedores de servicios de Internet (ISP, por sus siglas en inglés).

Además, Akamai implementa un amplio abanico de controles para la defensa contra ataques DDoS dentro de cada servidor, como los controles de frecuencia, las listas negras y el bloqueo por ubicación geográfica.

Resistencia a ataques DDoS en la red Prolexic

La red Prolexic es una de las redes de barrido de DDoS más avanzadas del mundo. Consta de 7 centros de barrido globales, más 3 Tbps de capacidad y un equipo formado por más de 150 profesionales de la seguridad que dan, a más de 500 clientes, protección frente a más de 200 ataques DDoS cada semana.

No dejamos de aumentar esta capacidad de protección frente a ataques DDoS. Cada centro de barrido posee varias conexiones de operadores de nivel 1. Disponemos de interconexión pública con más de 500 homólogos, así como análisis de tráfico de alto rendimiento y mitigación activa en varias capas de la pila OSI.

Resistencia a ataques DDoS en la infraestructura Fast DNS

Akamai ofrece un servicio de DNS autoritativo parecido al servicio de DNS gestionado por Dyn. Al diseñar Fast DNS, Akamai no solo se ocupó del rendimiento, sino también de garantizar la disponibilidad y la resistencia en caso de ataques DDoS. Hemos dividido nuestra infraestructura de Fast DNS en 20 nubes DNS individuales, cada una de ellas diseñada con fines específicos de disponibilidad. Luego, distribuimos los servidores de nombres asignados a nuestros clientes por las distintas nubes DNS para minimizar la repercusión que los ataques DDoS contra un cliente de Akamai puedan tener en los demás.

Dentro de cada nube DNS, Akamai despliega grupos de servidores de nombres, a fin de reducir al mínimo en la red global el impacto de los ataques localizados, por ejemplo, desplegando servidores de nombres directamente en los ISP de los usuarios finales para garantizar la prestación del servicio.

Además, Akamai mantiene controles adicionales para la defensa contra ataques DDoS, como la limitación de la frecuencia y la admisión, por medio de listas blancas, de solicitudes de DNS.

Conclusión

Akamai lleva cerca de dos décadas actuando contra ataques DDoS, protegiendo a los clientes y manteniendo la disponibilidad de las infraestructuras, incluso cuando se han producido los mayores ataques DDoS del momento. Akamai continúa investigando las amenazas nuevas y publicando estudios al respecto, como el aviso sobre amenaza publicado en agosto de 2016 en relación con la denominada Botnet Mirai. Seguimos desarrollando nuestra plataforma y nuestros procedimientos para ir siempre por delante de quienes tienen intenciones aviesas.

Cuanto mayores son los ataques DDoS, más nos empeñamos en supervisar nuestra red, así como en prever los requisitos y en proporcionar la capacidad precisa para mitigarlos.

A medida que aumenta la complejidad de los ataques DDoS, seguimos aplicando cuanto hemos aprendido defendiendo a todos nuestros clientes para conseguir protecciones más resistentes. Mantenemos el compromiso de proporcionar a los clientes de Akamai la plataforma más sólida del sector.

Revisión de su propia resistencia integral frente a ataques DDoS

Si desea recibir la ayuda de Akamai para hacer un análisis integral de la resistencia de su infraestructura y orientación sobre la conformidad de su configuración con nuestras prácticas recomendadas, póngase en contacto con nuestro departamento de servicios profesionales y solicite una consulta con nuestros arquitectos de seguridad empresarial.

1,2. Pollard, Jeff, Blankenship, Joseph y Cser, Andras: "Quick Take: Poor Planning, Not An IoT Botnet, Disrupted The Internet: Dyn Outage Underscores The Need To Plan For Failure", 24 de octubre de 2016. Forrester Research

Akamai FASTER FORWARD