ATAQUES DE REFLEXIÓN VÍA MEMCACHED:
UNA NUEVA ERA DE ATAQUES DDoS

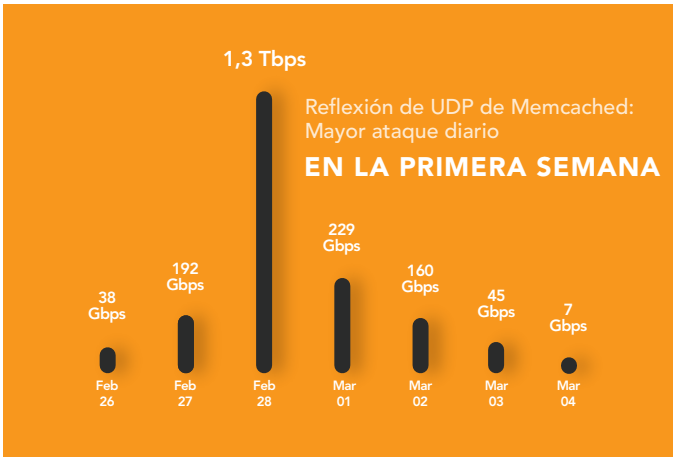
El volumen de las ofensivas DDoS se duplicó a comienzos de 2018, cuando los atacantes descubrieron y pusieron en marcha un nuevo método de amplificación y reflexión masivas de DDoS que tiene el potencial de multiplicar los recursos de ataque por medio millón. El vector de ataque, conocido como *reflexión de UDP de Memcached*, aprovecha recursos expuestos libremente en Internet, sin necesidad de recurrir a malware ni botnets.

El 28 de febrero de 2018, un cliente de Akamai fue testigo del mayor ataque DDoS, que registró el récord histórico de 1,3 terabits por segundo (Tbps) de tráfico de DDoS de reflexión en Memcached. Este volumen supone el doble que el de los ataques DDoS de mayor envergadura procedentes de la botnet Mirai del Internet de las cosas (IoT).

Prolexic, el servicio de Akamai para la protección ante DDoS, mitigó al instante la colosal acometida nada más recibir el tráfico de red del cliente, mediante la filtración de todo el tráfico procedente del puerto predeterminado usado por Memcached, una herramienta de código abierto destinada al almacenamiento de datos en caché. El tráfico se devolvió a la red del cliente totalmente limpio, tras pasar por los centros de barrido de DDoS de Akamai ubicados en Europa, EE. UU y Asia, y sin que se produjera ningún contratiempo en las operaciones del cliente.

El sistema Memcached, que hasta ahora solía emplearse para mejorar los tiempos de respuesta de las consultas de discos y bases de datos, se ha convertido en un arma cibernética que los atacantes aprovechan en sus técnicas de DDoS de reflexión. El primer caso de DDoS atribuido a la reflexión de Memcached se detectó solo dos días antes del ataque masivo. Cuando se produjo el ataque de 1,3 Tbps, Akamai ya había puesto en marcha medidas de mitigación para proteger al instante contra ataques de Memcached dirigidos a sus clientes.

La primera semana, se detectaron 19 ataques DDoS de reflexión de Memcached dirigidos a clientes de Akamai de distintos sectores.



Colosales tasa de paquetes y factor de amplificación de 500 000

La reflexión de Memcached presenta un tremendo factor de amplificación: una solicitud de 210 bytes podría dirigir una respuesta de 100 MB al objetivo. De forma predeterminada, los datos de Memcached se distribuyen a gran velocidad: Akamai midió una tasa de 127 millones de paquetes por segundo (Mpps) durante el ataque récord.

En un servidor de Internet sin protección que, además, tenga activado de forma predeterminada el protocolo de comunicación UDP, Memcached distribuye los datos a cualquiera que los solicite, incluidas direcciones IP falsificadas. En el ataque de 1,3 Tbps participaron miles de servidores en más de 1000 ASN, y cada uno de ellos distribuyó, de media, casi 1 Gbps de tráfico de ataques. Los estudios estiman que hay más de 90 000 servidores de Memcached en Internet, y 50 000 de ellos serían actualmente vulnerables a su uso como reflectores.

Expectativas de más ataques DDoS de extorsión y vía Memcached

Tal como han podido observar los profesionales de la seguridad con la constante popularidad de otros vectores de DDoS de reflexión, depender de administradores remotos del sistema a la hora de aplicar parches, reconfigurar o eliminar servidores vulnerables no ofrece unos resultados inmediatos. Y debemos prepararnos para recibir más ataques DDoS de Memcached en el futuro.

Con los ataques DDoS de reflexión de este tipo, los atacantes no necesitan malware para infectar y controlar los bots de una botnet: hasta los ciberdelincuentes menos expertos pueden lanzar una ofensiva. Akamai ha observado un incremento en los análisis destinados a identificar servidores de Memcached vulnerables. Los atacantes explotarán cada vez más servidores de Memcached para generar ataques DDoS de cualquier tamaño. Además, se están usando cargas útiles de datos de Memcached para distribuir mensajes con fines de extorsión, a lo que Akamai recomienda no ceder en ningún caso.

Los ataques DDoS saturan los canales de red local

Aparte de un pequeño número de organizaciones que disponen de un correcto sistema de mitigación contra ataques DDoS basado en la nube y de un proveedor de red de distribución de contenido (CDN) como Akamai, o de grandes proveedores de servicios, muy pocas organizaciones tienen suficiente capacidad de red para seguir adelante con sus operaciones mientras tienen que hacer frente a grandes ataques DDoS, y menos aún cuando se tratan de ofensivas de tal calibre. Al saturarse los canales de red local al centro de datos y los dispositivos de enrutamiento en el perímetro, no es posible mitigar los ataques DDoS in situ.

La importancia de planificar la mitigación de ataques DDoS

El cliente de Akamai afectado por este ataque DDoS récord estaba bien preparado y solo experimentó una interrupción de 10 minutos antes de desviar su tráfico a Akamai para que mitigara la ofensiva. Había contratado previamente el servicio de protección contra DDoS Prolexic, y se había desarrollado y practicado un runbook de DDoS, por lo que el personal sabía qué hacer y a quién dirigirse. Se supervisó el tráfico de red y, tras identificar la anomalía, los responsables desviaron todo el tráfico de red a Akamai en tan solo cinco minutos.

Por qué Akamai: diseño perfecto para la resistencia a los ataques DDoS

En Akamai protegemos a nuestros clientes frente a ataques DDoS con nuestra CDN, la red Prolexic y la infraestructura distribuida Fast DNS. No dejamos de invertir en mejorar la resistencia a los ataques DDoS de esas plataformas.

En el ámbito general, en Akamai, nuestro modelo de planificación de la capacidad parte de los mayores ataques DDoS que podemos verificar 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. De este modo, somos capaces de mitigar los ataques DDoS más sofisticados y de mayor envergadura hasta cuando duplican su tamaño, como sucedió en este caso.

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

Resistencia a ataques DDoS en la red de distribución de contenido

Aparte de la capacidad, diseñamos nuestra CDN de modo que ofrezca disponibilidad y resistencia en cualesquiera condiciones adversas, no solo en caso de un ataque DDoS. Con más de 220 000 servidores desplegados en todo el mundo, la CDN de Akamai se adapta al estado de cada servidor y desvía el tráfico de los usuarios de forma automática para eludir las interrupciones y congestiones. Cada servidor cuenta con defensas contra DDoS, como controles de tasa, listas negras y bloqueo por ubicación geográfica.

Resistencia a ataques DDoS en la red Prolexic

La red Prolexic ofrece uno de los servicios de barrido de DDoS más avanzados del mundo. Consta de 7 centros de barrido globales, más de 3,5 Tbps de capacidad y un equipo formado por más de 150 profesionales de la seguridad que brindan protección frente a miles de ataques DDoS cada mes. Cada centro de barrido posee varias conexiones de operadores de nivel 1 y una 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. No dejamos de aumentar esta capacidad de protección frente a ataques DDoS.

Resistencia a ataques DDoS en la infraestructura Fast DNS

Akamai opera un servicio de DNS autoritativo, Fast DNS, que ofrece alta disponibilidad, rapidez y resistencia frente a DDoS. Además, distribuimos los servidores de nombres asignados a nuestros clientes por más de 20 nubes de DNS segmentadas, para minimizar la repercusión que los ataques DDoS contra un cliente de Akamai pueden tener en los demás. Los grupos de servidores de nombres y los controles adicionales reducen al mínimo el impacto de los ataques DDoS localizados.

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. En Akamai seguimos investigando las amenazas nuevas y publicando estudios al respecto, así como desarrollando nuestra plataforma y nuestros procedimientos para ir siempre por delante de quienes tienen intenciones aviesas. Ponemos en práctica todo lo que aprendemos al defender a nuestros clientes para mejorar constantemente nuestros sistemas de protección. Mantenemos el compromiso de proporcionar a los clientes de Akamai la plataforma más sólida del sector.

Revisión de su propia resistencia frente a ataques DDoS

Si desea contar con la ayuda de Akamai para revisar la resistencia de su infraestructura, póngase en contacto con nuestro **departamento de Servicios Profesionales** para obtener asesoramiento de la mano de nuestros responsables de Arquitectura de Seguridad.

Puede obtener más información en **https://www.akamai.com/memcached.**

Akamai