KASPERSKY DDoS PROTECTION

Protección de su empresa contra las pérdidas financieras y de prestigio con Kaspersky DDoS Protection

Un ataque Distribuido de denegación de servicio (DDoS) es una de las armas más populares en el arsenal de los cibercriminales. Tiene como finalidad impedir a los usuarios regulares el acceso normal a sistemas de información, como sitios web o bases de datos. Detrás del inicio de un ataque DDoS pueden existir diferentes motivos, que van desde el vandalismo cibernético hasta las prácticas de competencia desleal o, incluso, la extorsión.

La industria moderna de DDoS es una estructura de varias capas. Incluye a las personas que encargan los ataques, los creadores de botnets que ponen sus recursos a disposición de los atacantes, intermediarios que coordinan los ataques y conversan con los clientes y personas que organizan los pagos de todos los servicios prestados. Cualquier nodo de red disponible en Internet se puede convertir en un objetivo, ser utilizado como un servidor específico, un dispositivo de red o una dirección en desuso en la subred de la víctima.

Existen dos situaciones comunes para efectuar ataques DDoS: enviar directamente solicitudes al recurso atacado desde un gran número de bots o iniciar un ataque DDoS por amplificación a través de servidores disponibles para el público que contienen vulnerabilidades de software. En la primera situación, los cibercriminales convierten una gran cantidad de computadoras en "zombies" controlados remotamente que luego siguen las órdenes de su amo y envían solicitudes de manera simultánea al sistema informático de la víctima (realizan un "ataque distribuido"). En ocasiones, hackers activistas reclutan a un grupo de usuarios, les suministran un software especial diseñado para realizar ataques DDoS y les comunican la orden de atacar un objetivo.

En la segunda situación que involucra un ataque por amplificación, se pueden utilizar servidores alquilados de un centro de datos en lugar de bots. Por lo general, se usan servidores públicos con software vulnerable para lograr resultados más óptimos. En la actualidad, se pueden utilizar servidores DNS (sistema de nombres de dominio) o servidores NTP (protocolo de tiempo de red). Un ataque se amplifica al falsificar direcciones IP de retorno y enviar una solicitud breve a un servidor que requiere una respuesta mucho más larga. La respuesta recibida se envía a la dirección IP falsificada que pertenece a la víctima.

Situaciones de ataques DDoS

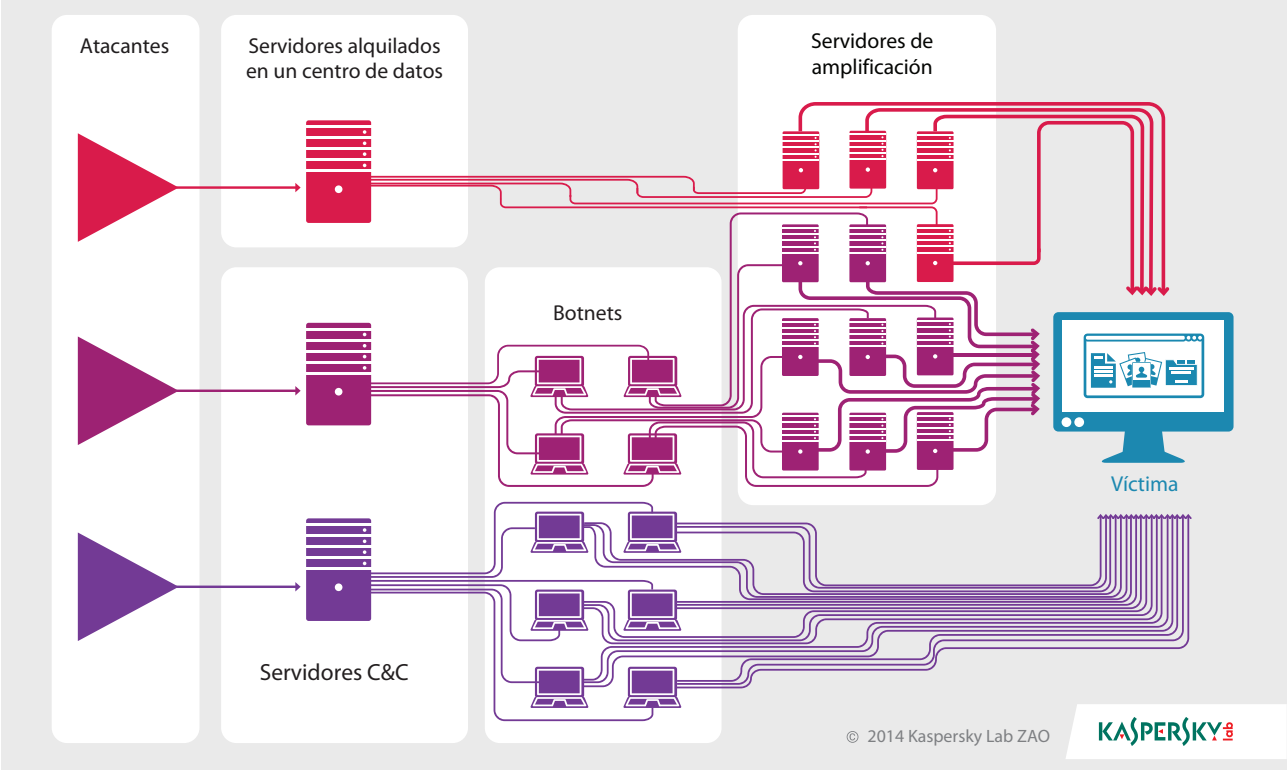

Figura 1. Diagrama de flujo de las versiones más populares de ataques DDoS

Existe otro factor que aumenta la peligrosidad de la situación. Debido a que hay tanto malware en circulación y los cibercriminales han creado tantos botnets, prácticamente cualquier persona puede iniciar este tipo de ataque. Los cibercriminales publicitan sus servicios afirmando que cualquier persona puede retirar un sitio especificado por una tarifa de solo $50 al día. Los pagos normalmente se realizan en criptomoneda, por lo que es casi imposible hacer seguimiento de los pedidos a través de flujos de efectivo.

Estos precios asequibles dan a entender que cualquier recurso en línea puede considerarse un objetivo para un ataque DDoS. Esto no se limita a los recursos de Internet de organizaciones grandes y famosas. Es más difícil causar daño a recursos web propiedad de grandes empresas, pero si estos dejan de estar disponibles, el costo de la interrupción será mucho mayor. Además de las pérdidas directas como resultado de oportunidades de negocios perdidas (como las ventas electrónicas), las empresas pueden enfrentar multas por incumplir sus obligaciones y gastos asociados a medidas adicionales para protegerse de otros ataques. Por último, pero igualmente importante, la reputación de la empresa puede verse perjudicada, lo que causará que pierda clientes existentes o potenciales.

El costo total depende del tamaño de la empresa, el segmento de la industria al que presta servicio y el tipo de servicio que fue objeto del ataque. Según los cálculos efectuados por la empresa de análisis IDC, una hora de interrupción de un servicio en línea puede costar a una empresa entre $10.000 y $50.000.

Métodos para contrarrestar los ataques DDoS

Existen docenas de empresas en el mercado que ofrecen servicios para protegerse de los ataques DDoS. Algunas instalan dispositivos en la infraestructura informática del cliente, otras utilizan capacidades dentro de proveedores ISP y otras canalizan el tráfico a través de centros de limpieza dedicados. Sin embargo, todos estos enfoques se adhieren al mismo principio: filtrar el tráfico basura, es decir, el tráfico generado por los cibercriminales.

La instalación de equipos de filtro en el lado del cliente se considera el método menos eficaz. En primer lugar, requiere personal capacitado especialmente dentro de la empresa para prestar servicio al equipo y ajustar su funcionamiento, lo que plantea costos adicionales. En segundo lugar, solo es eficaz contra ataques en el servicio y no hace nada para impedir ataques que saturan el canal de Internet. Un servicio en funcionamiento es inútil si es inaccesible desde la red. Como los ataques DDoS por amplificación están siendo cada vez más populares, está resultando mucho más fácil sobrecargar un canal de conexión.

Solicitar al proveedor que filtre el tráfico es una medida más confiable, puesto que existe un canal de Internet más amplio que es mucho más difícil de saturar. Por otra parte, los proveedores no se especializan en servicios de seguridad y solo filtran el tráfico basura más evidente, pasando por alto los ataques más sutiles. Un análisis cuidadoso de un ataque y una respuesta oportuna requieren un nivel adecuado de conocimientos y experiencia. Además, este tipo de protección lleva al cliente a depender de un proveedor específico y crea problemas si el cliente necesita utilizar un canal de datos de respaldo o cambiar de proveedor.

Como resultado, los centros de procesamiento especializados que implementan una combinación de varios métodos de filtro de tráfico se deben considerar el medio más eficaz para neutralizar los ataques DDoS.

Kaspersky DDoS Protection

Kaspersky DDoS Protection es una solución que protege contra todo tipo de ataques DDoS al utilizar una infraestructura distribuida de centros de limpieza de datos. La solución combina distintos métodos, que incluyen filtro de tráfico en el lado del proveedor, instalación de un dispositivo controlado en forma remota para analizar el tráfico al lado de la infraestructura del cliente y el uso de centros de limpieza especializados que poseen filtros flexibles. Además, el trabajo de la solución es monitoreado constantemente por los expertos de Kaspersky Lab, por lo que se logra detectar el inicio de cualquier ataque lo antes posible y los filtros se pueden modificar según sea necesario.

Kaspersky DDoS Protection en Modo activo

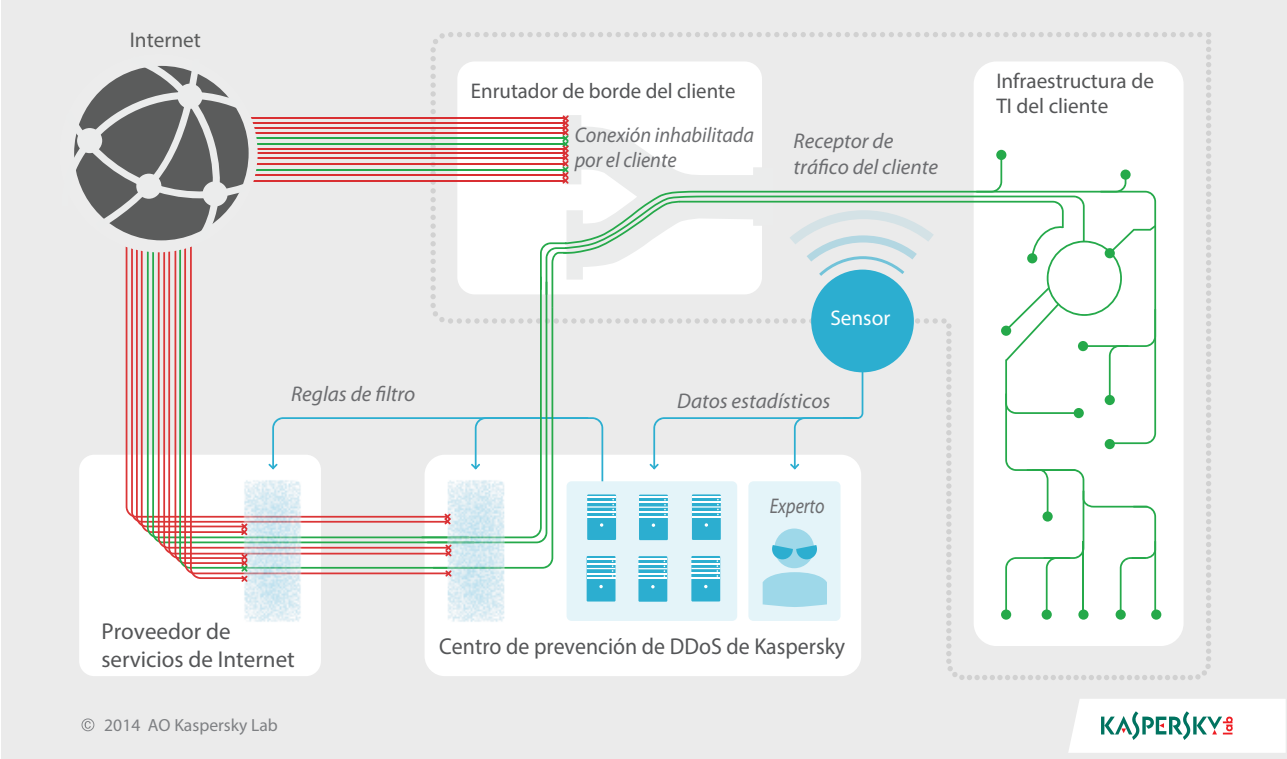

Figura 2. Kaspersky DDoS Protection: Diagrama de funcionamiento

Arsenal de Kaspersky Lab

Durante más de un década, Kaspersky Lab ha tratado con una amplia variedad de amenazas en línea. En el transcurso de ese período, los analistas de Kaspersky Lab han adquirido un nivel único de experiencia, que incluye una comprensión detallada de cómo funcionan los ataques DDoS. Los expertos de la empresa están siempre pendientes de los últimos avances que se producen en Internet, analizan los métodos más recientes para realizar ciberataques y mejoran nuestras herramientas de protección existentes. Gracias a la experiencia adquirida, pueden detectar un ataque DDoS tan pronto como se inicia y antes de que sature el recurso web de destino.

El segundo elemento de la tecnología de Protección DDoS de Kaspersky es un sensor instalado al lado de la infraestructura de TI del cliente. El sensor es un programa de software que se ejecuta en el sistema operativo Ubuntu y requiere un servidor x86 estándar. Analiza los tipos de protocolos utilizados, el número de bytes y paquetes de datos enviados, el comportamiento del cliente en el sitio web, es decir, los metadatos o información sobre los datos enviados. No redirige el tráfico a ningún lado ni modifica o analiza el contenido de todos los mensajes. A continuación, las estadísticas se envían a la infraestructura de Kaspersky DDoS Protection basada en nube, en la que se crea un perfil basado en estadísticas para cada cliente según los metadatos recopilados. En realidad, estos perfiles son registros de patrones típicos de intercambio de información de cada cliente. Se registran los cambios en los tiempos típicos de uso. Posteriormente, se analiza el tráfico; cada vez que el comportamiento de tráfico difiere del perfil basado en estadísticas, se puede considerar como la indicación de un ataque.

La clave de Kaspersky DDoS Protection está en sus centros de limpieza, que se ubican en las líneas troncales de Internet, en lugares como Frankfurt y Ámsterdam. Kaspersky Lab utiliza simultáneamente varios centros de limpieza, para poder dividir o redirigir el tráfico que es necesario limpiar. Los centros de procesamiento se unen en una infraestructura de información basada en nube común y los datos se mantienen dentro de esos límites. Por ejemplo, el tráfico web de clientes europeos no abandona el territorio europeo.

Otra forma clave de controlar el tráfico susceptible a DDoS es filtrarlo en el lado del proveedor. El ISP no solo suministra un canal de Internet, sino que también puede establecer una asociación tecnológica con Kaspersky Lab. De esa forma, Kaspersky DDoS Protection puede impedir el tráfico basura más evidente, que se utiliza en la mayoría de los ataques DDoS, lo más cerca posible de su punto de origen. Esto evita que los flujos se conviertan en un solo ataque poderoso y aligera la carga de los centros de limpieza, que se ven libres para filtrar tráfico basura más sofisticado.

Herramientas de redirección de tráfico

Para que la solución de seguridad funcione con eficacia, el primer requisito clave es configurar un canal de conexión entre los centros de limpieza y la infraestructura de TI del cliente. En Kaspersky DDoS Protection, estos canales se coordinan según el protocolo Encapsulación de ruta genérica. Estos se utilizan para crear un túnel virtual entre el centro de limpieza y los equipos de red del cliente, a través del cual se suministra el tráfico limpio al cliente.

La redirección de tráfico real se puede realizar utilizando uno de estos dos métodos: al anunciar la subred del cliente utilizando un protocolo de enrutamiento dinámico BGP o al modificar el registro de DNS al ingresar la URL del centro de limpieza. El primer método es preferible, puesto que puede redirigir el tráfico con mucha más rapidez y proteger de los ataques dirigidos a una dirección IP específica. No obstante, este método requiere que el cliente tenga un rango de direcciones que sea independiente del proveedor, como un bloque de direcciones IP suministrado por un registrador de Internet regional.

En lo que respecta al procedimiento de redirección real, no existe una gran diferencia entre los dos métodos. Si se usa el primer método, entonces los enrutadores BPG en el lado del cliente y en el centro de limpieza establecen una conexión permanente a través el túnel virtual; en caso de un ataque, se crea una nueva ruta desde el centro de limpieza al cliente. Cuando se usa el segundo método, al cliente se le asigna una dirección IP del repositorio de direcciones del centro de limpieza. Si se inicia un ataque, el cliente reemplaza la dirección IP en el registro DNS A por la dirección IP que le asignó el centro de limpieza. Después, todo el tráfico que llegue a la dirección del cliente se enviará primero al centro de limpieza. Sin embargo, para impedir que el ataque a la dirección IP antigua prosiga, el proveedor debe bloquear todo el tráfico entrante excepto por los datos que provienen del centro de limpieza.

Cómo funciona

En circunstancias normales, todo el tráfico de Internet se dirige directamente al cliente. Las medidas de protección comienzan a activarse no bien llega una señal del sensor. En algunos casos, los analistas de Kaspersky Lab detectan un ataque tan pronto como se inicia e informan al cliente. En este caso, las medidas de prevención se toman de manera anticipada. El experto en DDoS de Kaspersky Lab recibe una señal de que al cliente le está llegando tráfico que no coincide con el perfil estadístico. Si el ataque se confirma, entonces se notifica al cliente y se debe emitir la orden de redirigir el tráfico a los centros de limpieza (en algunos casos, puede existir un acuerdo con el cliente para que la redirección se inicie de manera automática).

Tan pronto como las tecnologías de Kaspersky Lab determinan el tipo de ataque, se aplican reglas de limpieza específicas para este tipo de ataque y recurso web. Algunas de las reglas, diseñadas para enfrentar el tipo más grave de ataques, se comunican a la infraestructura del proveedor y se aplican en enrutadores de propiedad del proveedor. El tráfico restante se entrega a los servidores del centro de limpieza y se filtra de acuerdo con varias señales características, como direcciones IP, datos geográficos, información de los encabezados HTTP, la corrección de los protocolos y el intercambio de paquetes SYN, etc.

El sensor sigue monitoreando el tráfico a medida que llega al cliente. Si sigue mostrando señales de un ataque DDoS, el sensor alerta al centro de limpieza y el tráfico se somete a un análisis exhaustivo de comportamiento y firmas. Con estos métodos es posible filtrar el tráfico malicioso según las firmas; por ejemplo, se puede bloquear por completo un tipo específico de tráfico o se pueden bloquear direcciones IP según criterios específicos observados. De esta manera, se filtran incluso los ataques más sofisticados, incluidos los ataques de saturación de HTTP. Estos ataques consisten en imitaciones de un usuario que visita un sitio web que, en realidad, son caóticas, mucho más rápidas de lo común y normalmente provienen de un batallón de computadoras zombie.

Los expertos de Kaspersky Lab monitorean todo el proceso utilizando una interfaz dedicada. Si un ataque es más complejo de lo habitual o es atípico, el experto puede intervenir, cambiar las reglas de filtro y reorganizar los procesos. Además, los clientes pueden ver cómo se ejecuta la solución y cómo se comporta el tráfico, utilizando su propia interfaz.

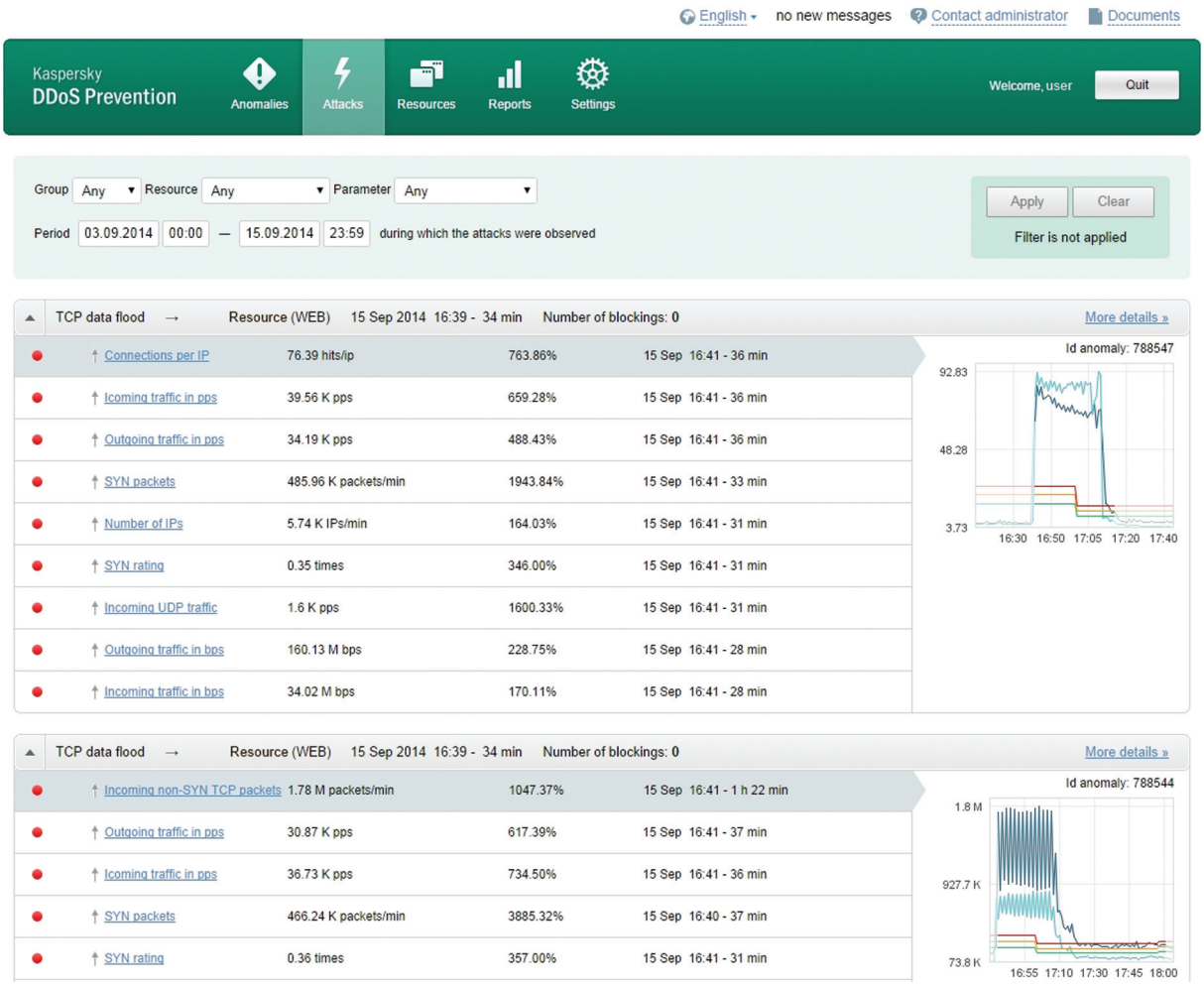

Figura 3. Captura de pantalla de la interfaz del cliente

Cuando termina el ataque, el tráfico se vuelve a dirigir a los servidores del cliente. Kaspersky DDoS Protection se revierte al modo de espera y el cliente recibe un informe detallado del ataque, que incluye datos detallados de cómo se desarrolló, gráficas que indican visualmente los parámetros medibles y la distribución geográfica de las fuentes del ataque.

Ventajas del enfoque de Kaspersky Lab

- Solo la redirección del tráfico a los centros de limpieza de Kaspersky Lab durante un ataque y el filtro del tráfico en el lado del proveedor ayudan de manera importante a reducir el costo para el cliente.
- Las reglas de filtro se desarrollan en forma individual para cada cliente según los servicios específicos en línea que deba proteger.
- Los expertos de Kaspersky Lab monitorean el proceso y ajustan con rapidez las reglas de filtrado cuando es necesario.
- La colaboración estrecha entre los expertos de Kaspersky DDoS Protection y los desarrolladores de Kaspersky Lab hace posible adaptar la solución en forma flexible y rápida según las circunstancias cambiantes.
- Para garantizar el nivel más alto posible de confiabilidad, Kaspersky Lab solo utiliza equipos y proveedores de servicios europeos en países europeos.
- Kaspersky Lab ha acumulado una vasta experiencia en la aplicación de esta tecnología en Rusia, donde protege con éxito a las principales instituciones financieras, organismos comerciales y gubernamentales, tiendas en línea, entre otros.

15 de marzo/Global