PROTECCIÓN CONTRA DDoS DE KASPERSKY

Protección para su empresa frente a pérdidas financieras y de reputación con la protección contra DDoS de Kaspersky

Un ataque de denegación de servicio distribuido (DDoS, del inglés "Distributed Denial of Service") es una de las armas más populares del arsenal de los cibercriminales. Su objetivo es hacer que los usuarios habituales no puedan acceder de forma normal a los sistemas de información tales como bases de datos o sitios web. Pueden existir diferentes motivos para el lanzamiento de ataques de DDoS, que van desde el cibergamberrismo hasta prácticas de competencia indeseables o incluso extorsión.

El moderno sector de DDoS es una estructura de varios niveles. Incluye a personas que encargan los ataques, los creadores del botnet que hacen que sus recursos estén disponibles, los intermediarios que organizan los ataques y hablan con los clientes, y las personas que organizan los pagos de todos los servicios prestados. Cualquier nodo de la red disponible en Internet puede convertirse en un objetivo, ya sea un servidor, un dispositivo de red o una dirección en desuso en la subred víctima.

Hay dos escenarios comunes para llevar a cabo ataques de DDoS: el envío de solicitudes directamente al recurso atacado desde un gran número de bots o el lanzamiento de un ataque amplificado de DDoS a través de servidores disponibles públicamente que contienen vulnerabilidades del software. En el primer escenario, los cibercriminales convierten un gran número de ordenadores en "zombis" controlados de forma remota que cumplen las órdenes del ordenador principal y envían simultáneamente solicitudes al sistema informático víctima (realizan un "ataque distribuido"). A veces, los activistas hackers reclutan un grupo de usuarios y les proporcionan un software especial diseñado para llevar a cabo ataques de DDoS y órdenes determinadas para atacar un objetivo.

En el segundo escenario de ataque amplificado, se pueden tomar prestados los servidores de un centro de datos en lugar de utilizar bots. Para la mejora normalmente se utilizan servidores públicos con software vulnerable. Hoy en día, se pueden utilizar tanto servidores DNS (sistema de nombres de dominio, del inglés "Domain Name System") como servidores NTP (protocolo de tiempo de redes, del inglés "Network Time Protocol"). Un ataque se amplifica mediante la falsificación de direcciones IP de devolución y el envío de 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.

Escenarios de ataque de DDoS

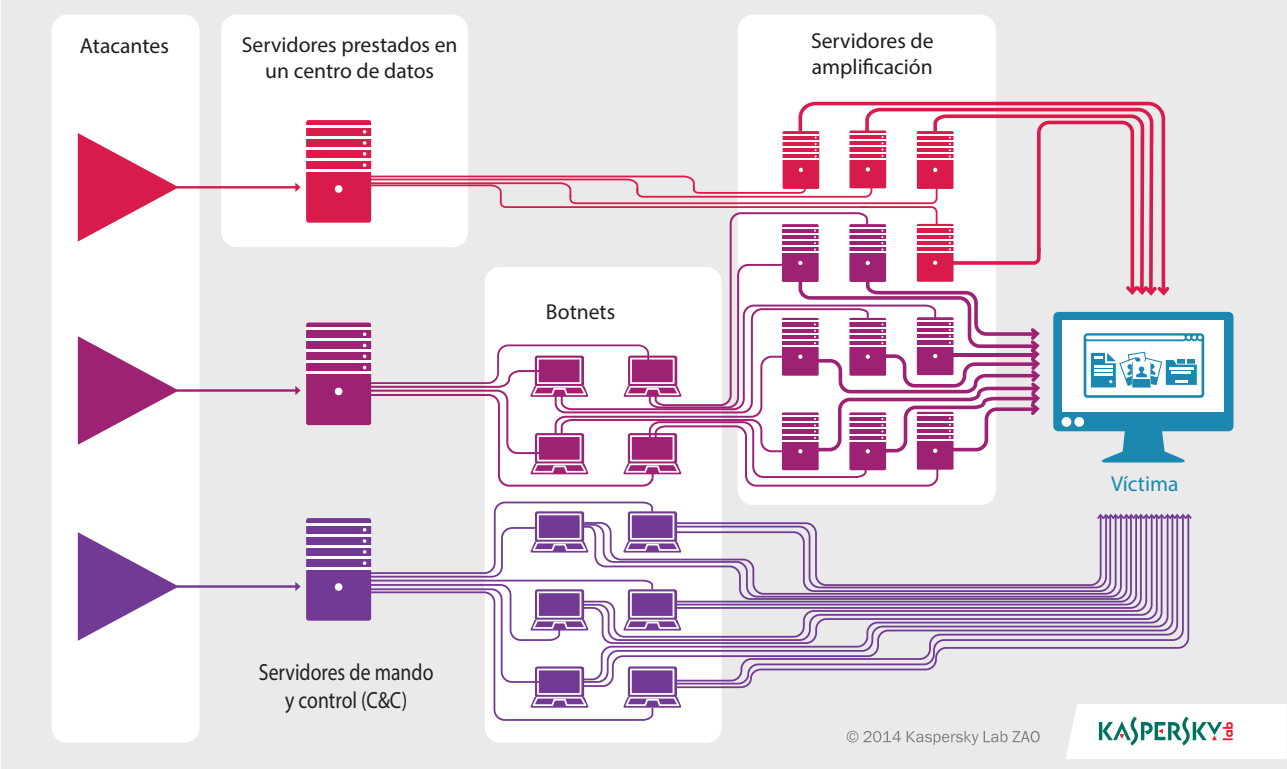

Figura 1. Diagrama de flujo de la mayoría de las versiones más populares de los ataques de DDoS

Existe otro factor que hace que la situación sea aún más peligrosa. Como existe mucho malware y los cibercriminales han creado tantos bots, casi cualquiera puede lanzar este tipo de ataque. Los cibercriminales hacen propaganda de sus servicios diciendo que cualquiera puede piratear un sitio específico por tan solo 50 dólares al día. Los pagos se suelen realizar en criptomoneda, por lo que es prácticamente imposible rastrear los pedidos a través de flujos de efectivo.

Los precios asequibles hacen que cualquier recurso online pueda ser blanco de un ataque de DDoS. Los ataques no se limitan a los recursos de Internet de las empresas grandes y famosas. Es más difícil dañar los recursos web que son propiedad de grandes empresas, pero si se consigue que no estén disponibles, el coste del tiempo de inactividad será mucho mayor. Además de las pérdidas directas a consecuencia de la pérdida de oportunidades de negocios (como las ventas electrónicas), las empresas pueden obtener multas por incumplimiento de sus obligaciones o el pago de gastos en relación con las medidas adicionales que tienen que implementar para protegerse de nuevos ataques. Por último, pero no por ello menos importante, la reputación de la empresa puede verse dañada, lo que hace que puedan perderse clientes existentes o futuros.

El coste total depende del tamaño de la empresa, el segmento del sector al que sirve y el tipo de servicio atacado. Según los cálculos de la empresa de análisis IDC, una hora de tiempo de inactividad de un servicio online puede costar a una empresa de 10 000 a 50 000 dólares.

Métodos para contrarrestar ataques de DDoS

Hay decenas de empresas en el mercado que ofrecen servicios para proteger contra los ataques de DDoS. Algunas instalan dispositivos en la infraestructura de información del cliente, otras utilizan capacidades en proveedores de servicios de Internet (ISP) y otras dirigen el tráfico a través de centros de limpieza especializados. No obstante, todos estos enfoques siguen el mismo principio: el filtrado del tráfico basura, es decir, tráfico creado por los cibercriminales.

La instalación de equipos de filtrado en el cliente se considera el método menos eficaz. En primer lugar, requiere personal especialmente formado dentro de la empresa para el mantenimiento de los equipos y el ajuste de su funcionamiento, lo que crea costes adicionales. En segundo lugar, solo es eficaz contra los ataques al servicio y no hace nada para impedir los ataques que asfixian el canal de Internet. Un servicio en funcionamiento no sirve de nada si no se puede acceder a este desde la red. A medida que los ataques de DDoS se hacen más populares, la sobrecarga de un canal de conexión se ha vuelto mucho más fácil.

Que el proveedor filtre el tráfico es más fiable, ya que es un canal más amplio de Internet y es mucho más difícil de asfixiar. Por otra parte, los proveedores no se especializan en servicios de seguridad y solo filtran el tráfico basura más obvio, pasando por alto los ataques más sutiles. Un análisis minucioso de un ataque y una respuesta rápida requieren la experiencia y los conocimientos adecuados. Además, este tipo de protección hace que el cliente dependa de un proveedor específico y crea dificultades en el caso de que el cliente necesite utilizar un canal de datos de copia de seguridad o cambiar su proveedor.

Como resultado, los centros de procesamiento especializados que implementen una combinación de varios métodos de filtrado de tráfico deberían considerarse la forma más eficaz de neutralizar los ataques de DDoS.

Protección contra DDoS de Kaspersky

Protección contra DDoS de Kaspersky es una solución que protege contra todo tipo de ataques de DDoS mediante una infraestructura distribuida de centros de limpieza de datos. La solución combina diferentes métodos, incluido el filtrado de tráfico por parte del proveedor, la instalación de un dispositivo controlado de forma remota para analizar tráfico junto a la infraestructura del cliente y el uso de centros de limpieza especializados con filtros flexibles. Además, los expertos de Kaspersky Lab supervisan constantemente el funcionamiento de la solución, por lo que el comienzo de cualquier ataque se puede detectar lo más rápido posible y los filtros se pueden modificar según sea necesario.

Protección contra DDoS de Kaspersky en modo activo

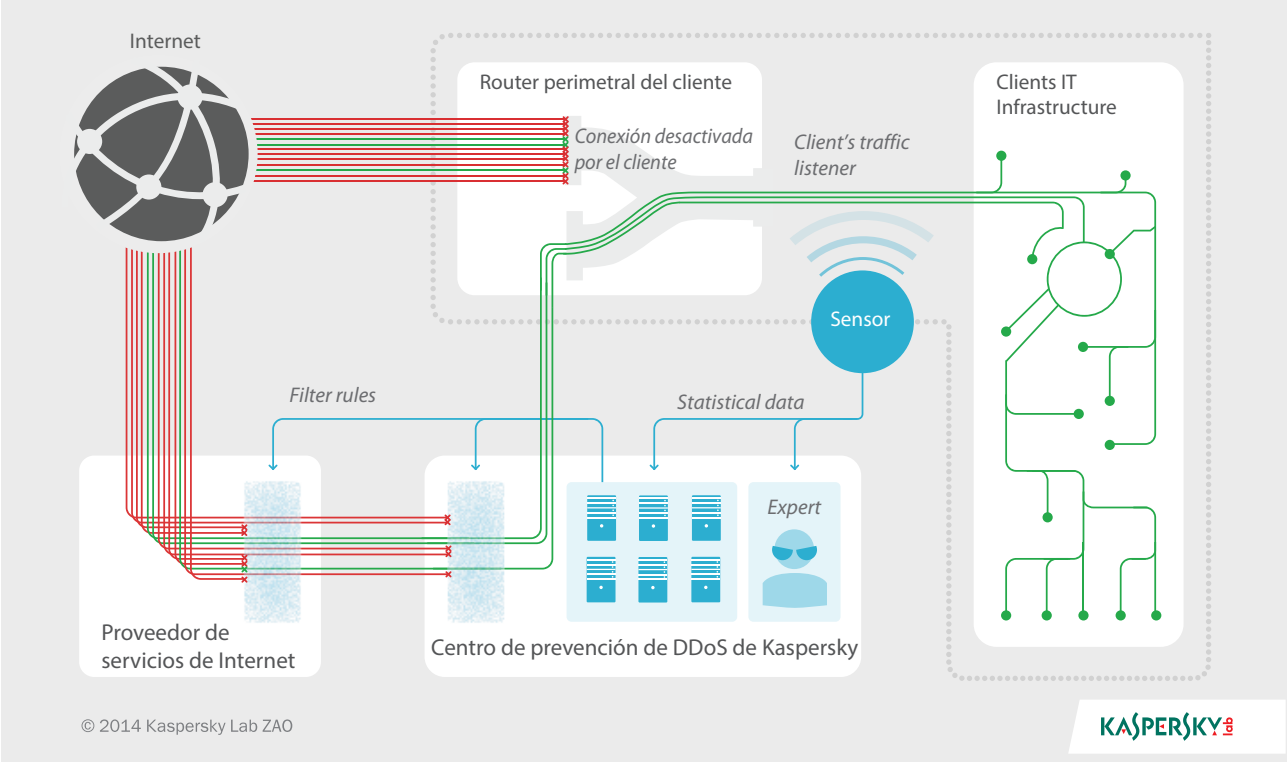

Figura 2. Protección contra DDoS de Kaspersky: diagrama de funcionamiento

Al arsenal de Kaspersky Lab

Durante más de una década, Kaspersky Lab ha resuelto con éxito una amplia gama de amenazas online. Durante ese tiempo, los analistas de Kaspersky Lab han adquirido un nivel único de experiencia, incluida una comprensión detallada de cómo funcionan los ataques de DDoS. Los expertos de la empresa vigilan constantemente los desarrollos más recientes que tienen lugar en Internet, analizan los últimos métodos de ciberataques y mejoran nuestras herramientas de protección actuales. Con esta experiencia al alcance de la mano, es posible detectar un ataque de DDoS tan pronto como se inicie y antes de que sature el recurso de la web objetivo.

El segundo elemento de la tecnología de protección contra DDoS de Kaspersky es un sensor instalado junto a la infraestructura de IT del cliente. El sensor es un componente 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 la información acerca de los datos enviados. No redirige el tráfico a ninguna parte ni lo modifica, así como tampoco analiza el contenido de los mensajes. Las estadísticas se distribuyen a continuación a la infraestructura de protección contra DDoS de Kaspersky en la nube, en la que se crea un perfil basado en las estadísticas para cada cliente en función de los metadatos. Estos perfiles son registros de patrones de intercambio de información habituales para cada cliente. Se registran los cambios en los momentos de uso habituales. Más adelante, el tráfico se analiza; si en cualquier momento el comportamiento del tráfico es diferente del que aparece en el perfil basado en las estadísticas, es posible que se trate de un ataque.

La piedra angular de la protección contra DDoS de Kaspersky son sus centros de limpieza. Estos están ubicados en las principales líneas troncales de Internet, en lugares como Frankfurt y Ámsterdam. Kaspersky Lab utiliza simultáneamente varios centros de limpieza, por lo que puede dividir o redirigir el tráfico que se debe limpiar. Los centros de procesamiento están unidos en una infraestructura de información común en la nube y los datos se encuentran dentro de esos límites. Por ejemplo, el tráfico web de los clientes europeos no abandona el territorio europeo.

Otra manera clave de controlar el tráfico de DDoS es que el proveedor lo filtre. El ISP no solo proporciona un canal de Internet, sino que también puede ser un partner tecnológico de Kaspersky Lab. Por lo tanto, la protección contra DDoS de Kaspersky puede cortar el tráfico basura más obvio que se utiliza en la mayoría de los ataques de DDoS, tan cerca de su punto de origen como sea posible. Esto evita que los flujos se integren en un solo ataque potente y alivia la carga de los centros de limpieza, que así pueden gestionar el tráfico basura más sofisticado.

Herramientas de redireccionamiento del tráfico

Para que la solución de seguridad funcione de forma eficaz, el primer requisito fundamental es el establecimiento de un canal de conexión entre los centros de limpieza y la infraestructura de IT del cliente. En la protección contra DDoS de Kaspersky, estos canales se organizan en función del protocolo de encapsulación de enrutamiento genérico. Se utilizan para crear un túnel virtual entre el centro de limpieza y el equipo de red del cliente, a través del cual se distribuye el tráfico limpio al cliente.

El redireccionamiento real del tráfico se puede hacer mediante uno de los dos métodos siguientes: mediante el anuncio de la subred del cliente a través de un protocolo de enrutamiento dinámico BGP, o bien mediante la modificación del registro de DNS a través de la introducción de la dirección URL del centro de limpieza. El primer método es preferible porque puede redirigir tráfico de forma mucho más rápida y proteger contra ataques que afectan directamente a una dirección IP específica. No obstante, este método necesita que el cliente tenga intervalos de direcciones independientes del proveedor, como un bloque de direcciones IP proporcionadas por un registro regional de Internet.

En cuanto al procedimiento de redireccionamiento real, hay poca diferencia entre los dos métodos. Si se utiliza el primer método, entonces los routers BPG del cliente y el centro de limpieza establecen una conexión permanente a través del túnel virtual; en caso de ataque, se crea una nueva ruta desde el centro de limpieza hasta el cliente. Cuando se utiliza el segundo método, al cliente se le asigna una dirección IP del grupo de direcciones del centro de limpieza. Si se inicia un ataque, el cliente sustituye la dirección IP en el registro DNS A por la dirección IP asignada por el centro de limpieza. Una vez realizada esta acción, todo el tráfico que llega a la dirección del cliente se envía primero al centro de limpieza. No obstante, para detener totalmente el ataque contra la dirección IP antigua, el proveedor debe bloquear todo el tráfico entrante excepto los datos procedentes del centro de limpieza.

Funcionamiento

En circunstancias normales, todo el tráfico de Internet pasa directamente al cliente. Las acciones protectoras comienzan tan pronto como se recibe 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 se pueden tomar medidas preventivas. El experto en DDoS de servicio en Kaspersky Lab recibe una señal que indica que el tráfico que llega al cliente no coincide con el perfil estadístico. Si el ataque se confirma, a continuación se notifica al cliente del ataque, quien debe dar la orden para redirigir el tráfico a los centros de limpieza (en algunos casos, puede que haya un acuerdo con el cliente para que el redireccionamiento se inicie automáticamente).

Tan pronto como las tecnologías de Kaspersky Lab determinan el tipo de ataque, se aplican las reglas de limpieza específicas para este tipo de ataque y el recurso web específico. Algunas de las reglas, diseñadas para tratar los tipos de ataques más básicos, se comunican a la infraestructura del proveedor y se aplican en los routers que son propiedad del proveedor. El tráfico restante se distribuye a los servidores del centro de limpieza y se filtra en función de una serie de señales características, como las direcciones IP, los datos geográficos, la información sobre los encabezados HTTP, la exactitud de los protocolos y el intercambio de paquetes SYN, etc.

El sensor continúa supervisando el tráfico mientras llega al cliente. Si aún muestra señales de un ataque de DDoS, el sensor envía una alerta al centro de limpieza y el tráfico se somete a un análisis profundo del comportamiento y las firmas. Con estos métodos, el tráfico malicioso se puede filtrar en función de las firmas, es decir, se puede bloquear completamente un tipo específico de tráfico o solo determinadas direcciones IP en función de criterios específicos observados. De esta manera, incluso los ataques más sofisticados se filtran, incluidos un ataque de saturación de HTTP. Estos ataques funcionan como imitaciones de las visitas de un usuario a un sitio web, pero en realidad son caóticas, extrañamente rápidas y generalmente proceden de un regimiento de ordenadores zombi.

Los expertos de Kaspersky Lab supervisan todo el proceso mediante el uso de una interfaz especializada. Si el ataque es más complicado de lo habitual o atípico, el experto puede intervenir, cambiar las reglas de filtrado y reorganizar los procesos. Los clientes también pueden observar cómo funciona la solución y cómo se comporta el tráfico a través de su propia interfaz.

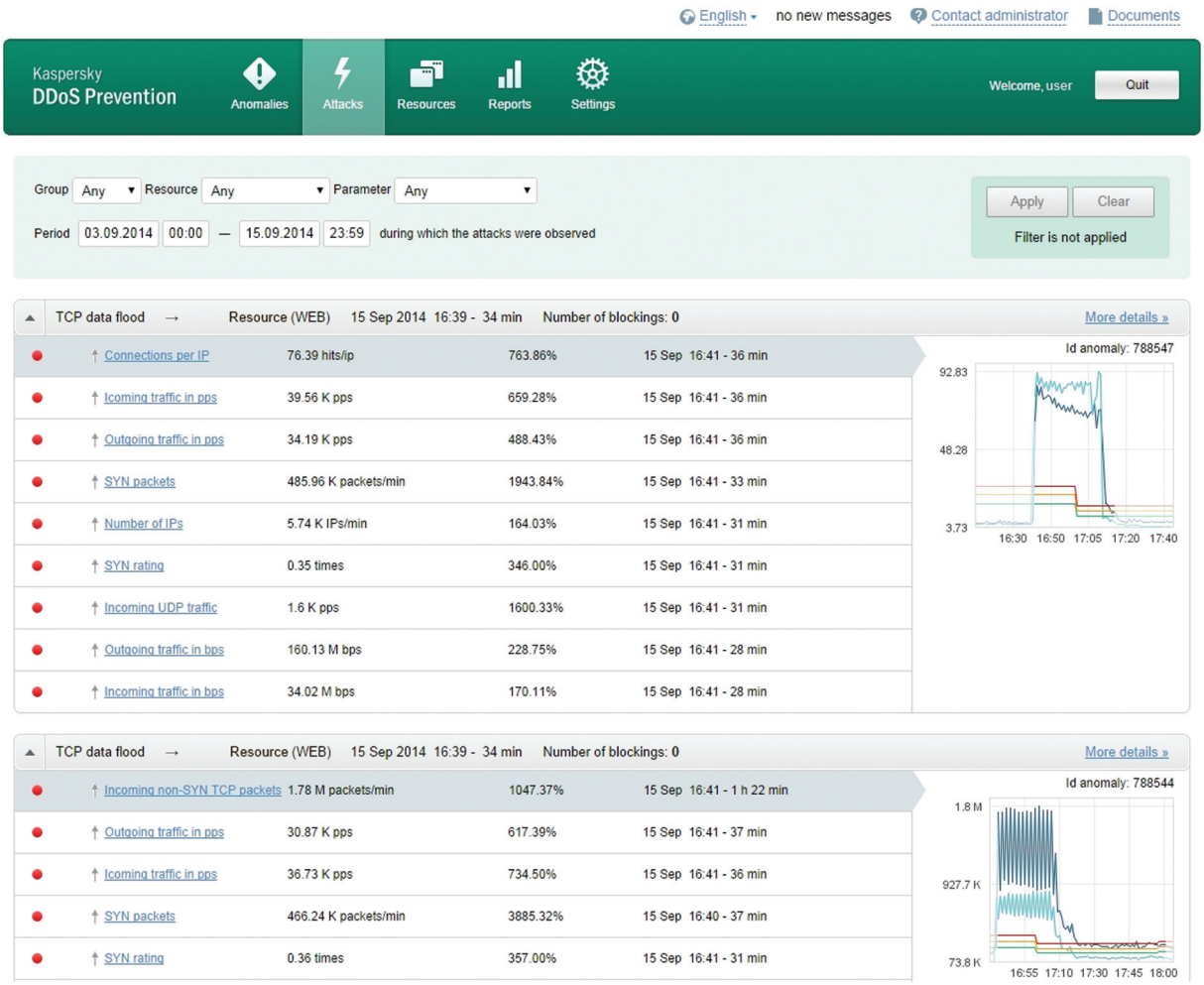

Figura 3. Captura de pantalla de la interfaz del cliente

Cuando el ataque ha finalizado, el tráfico se dirige de nuevo a los servidores del cliente. La protección contra DDoS de Kaspersky vuelve al modo en espera y el cliente recibe un informe detallado del ataque, incluida una descripción detallada de cómo se ha desarrollado, gráficos que trazan los parámetros evaluables y la distribución geográfica de las fuentes del ataque.

Ventajas del enfoque de Kaspersky Lab

- El redireccionamiento del tráfico a los centros limpieza de Kaspersky Lab durante un ataque y el filtrado del tráfico por parte del proveedor son los únicos elementos que ayudan a reducir significativamente el coste al cliente.
- Las reglas de filtrado se desarrollan de forma personalizada para cada cliente en función de los servicios online específicos que deben protegerse.
- Los expertos de Kaspersky Lab supervisan el proceso y ajustan rápidamente las reglas de filtrado cuando es necesario.
- La estrecha colaboración entre los expertos de la protección contra DDoS de Kaspersky y los desarrolladores de Kaspersky Lab hace posible la adaptación de la solución de forma rápida y flexible en respuesta a las circunstancias cambiantes.
- Para garantizar el máximo nivel de fiabilidad, Kaspersky Lab solo utiliza equipos y proveedores de servicios europeos en los países europeos.
- Kaspersky Lab ha acumulado una vasta experiencia mediante la aplicación de esta tecnología en Rusia, donde protege con éxito importantes instituciones financieras, agencias comerciales y gubernamentales, tiendas online, etc.

Marzo de 2015/Global