KASPERSKY DDoS PROTECTION

Proteja a sua empresa contra perdas financeiras e de reputação com o Kaspersky DDoS Protection

Um ataque DDoS (Distributed Denial of Service, Negação de Serviço Distribuído) é uma das mais populares armas no arsenal dos cibercriminosos. Ele torna o acesso convencional a sistemas de informação, como sites ou bancos de dados, impossível para usuários normais. Pode haver diferentes motivos por trás da execução de ataques DDoS, que vão desde "vandalismo cibernético" a práticas de concorrência sujas ou até mesmo extorsão.

A moderna indústria de DDoS é uma estrutura em várias camadas. Ela inclui pessoas que promovem ataques, os criadores de botnet que disponibilizam seus recursos, intermediários que organizam ataques e que mantêm contato com os clientes, e as pessoas que providenciam pagamentos para todos os serviços oferecidos. Qualquer nó de rede disponível na Internet pode se tornar um alvo, seja ele um servidor específico, um dispositivo de rede ou um endereço em desuso na sub-rede da vítima.

Há dois cenários comuns para a realização dos ataques DDoS: enviar solicitações diretamente para o recurso atacado a partir de um grande número de bots, ou executar um ataque de amplificação de DDoS através de servidores disponíveis publicamente que contêm vulnerabilidades de software. No primeiro cenário, os cibercriminosos transformam uma infinidade de computadores em "zumbis" controlados remotamente que, em seguida, seguem o comando do mestre e enviam solicitações simultaneamente para o sistema de computação da vítima (conduzindo um "ataque distribuído"). Às vezes, um grupo de usuários é recrutado por hacktivistas, dotados de software especial criado para realizar ataques DDoS e com ordens para atacar um alvo.

No segundo cenário envolvendo um ataque de amplificação, servidores alugados fora de um centro de dados podem ser usados em vez de bots. Servidores públicos com software vulnerável normalmente são usados para intensificar o ataque. Atualmente, servidores DNS (Domain Name System, Sistema de Nome de Domínio) ou NTP (Network Time Protocol, Protocolo de Tempo de Rede) podem ser utilizados. Um ataque é amplificado por meio da falsificação de endereços IP de retorno e do envio uma breve solicitação para um servidor que requer uma resposta muito mais longa. A resposta recebida é enviada para o endereço IP falso que pertence à vítima.

Cenários de ataque DDoS

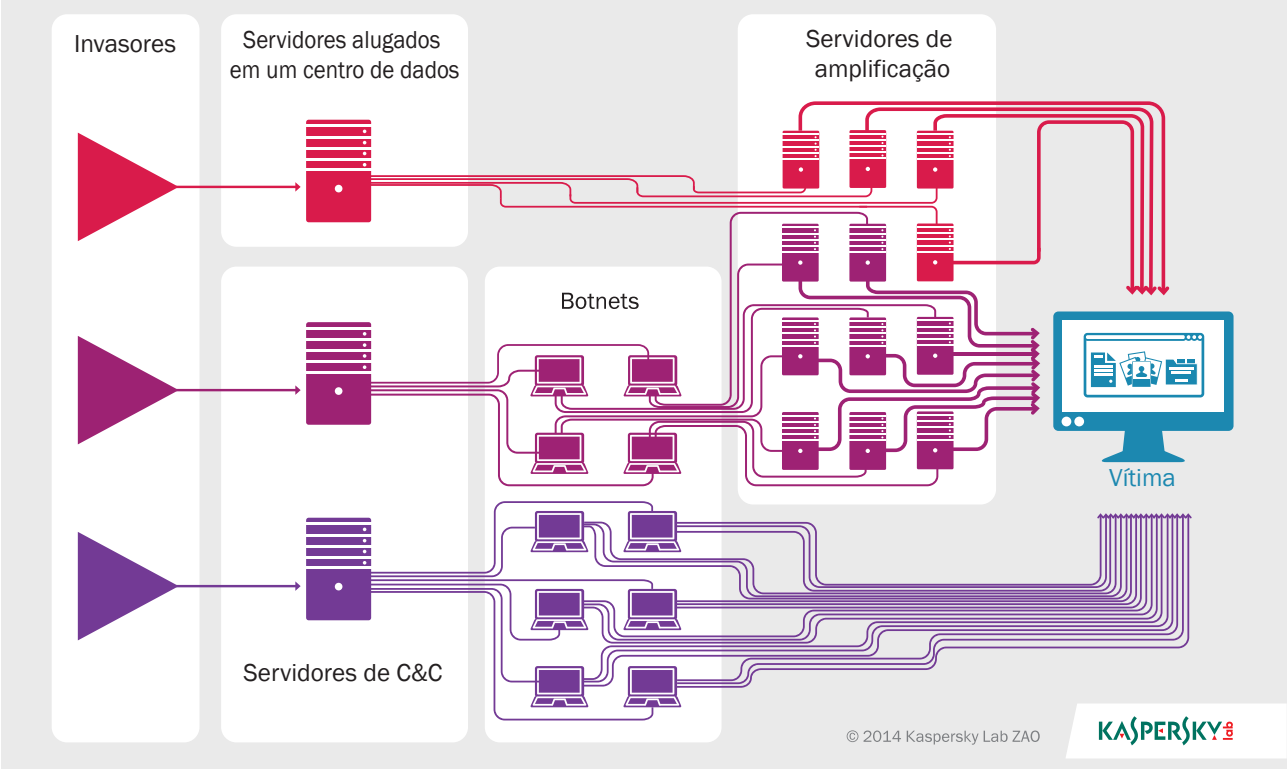

Figura 1. Diagrama de fluxo das versões mais populares dos ataques DDoS

Há outro fator que torna a situação ainda mais perigosa. Visto que existem muitos malwares, e os cibercriminosos criaram tantos botnets, quase qualquer indivíduo pode executar esse tipo de ataque. Criminosos virtuais anunciam seus serviços dizendo que qualquer pessoa pode derrubar um site específico por apenas US$ 50 por dia. Os pagamentos geralmente são feitos em criptomoeda, por isso é quase impossível descobrir os pedidos através de fluxos de caixa.

Preços acessíveis significam que qualquer recurso on-line pode ser alvo de um ataque DDoS. Não é algo limitado aos recursos da Internet de organizações grandes e famosas. É mais difícil provocar danos a recursos da Web pertencentes a grandes empresas, mas se eles ficarem indisponíveis, o custo da paralisação será muito maior. Além das perdas diretas que resultam da perda de oportunidades de negócios (como vendas eletrônicas), as empresas podem enfrentar multas pelo descumprimento de suas obrigações ou despesas relacionadas a medidas adicionais para proteger a si mesmas contra ataques futuros. Por último, mas não menos importante, a reputação da empresa pode ser danificada, fazendo com que ela perca clientes existentes ou futuros.

O custo total depende do tamanho da empresa, do segmento da indústria que ela atende e do tipo de serviço sob ataque. De acordo com os cálculos da empresa avaliadora, IDC, uma hora de inatividade de um serviço on-line pode custar à empresa US$ 10.000 a US$ 50.000.

Métodos para combater ataques DDoS

Existem dezenas de empresas disponíveis no mercado que fornecem serviços para proteger contra ataques DDoS. Algumas instalam aparelhos na infraestrutura de informação do cliente, algumas usam recursos dentro dos provedores ISP e outras "canalizam" o tráfego através de centros de limpeza dedicados. No entanto, todas essas abordagens seguem o mesmo princípio: o tráfego de lixo eletrônico, ou seja, o tráfego criado por criminosos virtuais, não se enquadra nesse caso.

Instalar equipamentos de filtragem no cliente é considerado o método menos eficaz. Em primeiro lugar, ele requer técnicos com a formação adequada dentro da empresa para a manutenção dos equipamentos e o ajuste da sua operação, criando custos adicionais. Em segundo lugar, ele só é eficaz contra ataques no serviço e não faz nada para impedir ataques que "engarrafam" o canal da Internet. Um serviço operante não será útil se não puder ser acessado a partir da Internet. À medida que ataques DDoS amplificados ficaram mais populares, tornou-se muito mais fácil sobrecarregar um canal de conexão.

É mais confiável fazer com que o provedor filtre o tráfego, pois há um canal da Internet mais amplo e ele é muito mais difícil de ser obstruído. Por outro lado, os provedores não são especializados em serviços de segurança e filtram apenas o tráfego de lixo eletrônico mais óbvio, negligenciando ataques mais tênues. Uma análise cuidadosa de um ataque e uma resposta imediata requerem o devido conhecimento e experiência. Além disso, esse tipo de proteção torna o cliente dependente de um provedor específico e cria dificuldades se o cliente precisar utilizar um canal de dados reserva ou mudar seu provedor.

Como resultado disso, centros de processamento especializados que implementam uma combinação de diversos métodos de filtragem de tráfego devem ser considerados como o meio mais eficaz para neutralizar ataques DDoS.

Kaspersky DDoS Protection

O Kaspersky DDoS Protection é uma solução que protege contra todos os tipos de ataques DDoS usando uma infraestrutura distribuída de centros de limpeza de dados. A solução combina diferentes métodos, incluindo a filtragem de tráfego no lado do provedor, a instalação de um aparelho controlado remotamente para analisar o tráfego próximo da infraestrutura do cliente, e o uso de centros de limpeza especializados com filtros flexíveis. Além disso, o trabalho da solução é constantemente monitorado pelos especialistas da Kaspersky Lab, para que o surgimento de qualquer ataque possa ser detectado o mais rápido possível, e para que os filtros possam ser modificados conforme necessário.

Kaspersky DDoS Protection em Modo Ativo

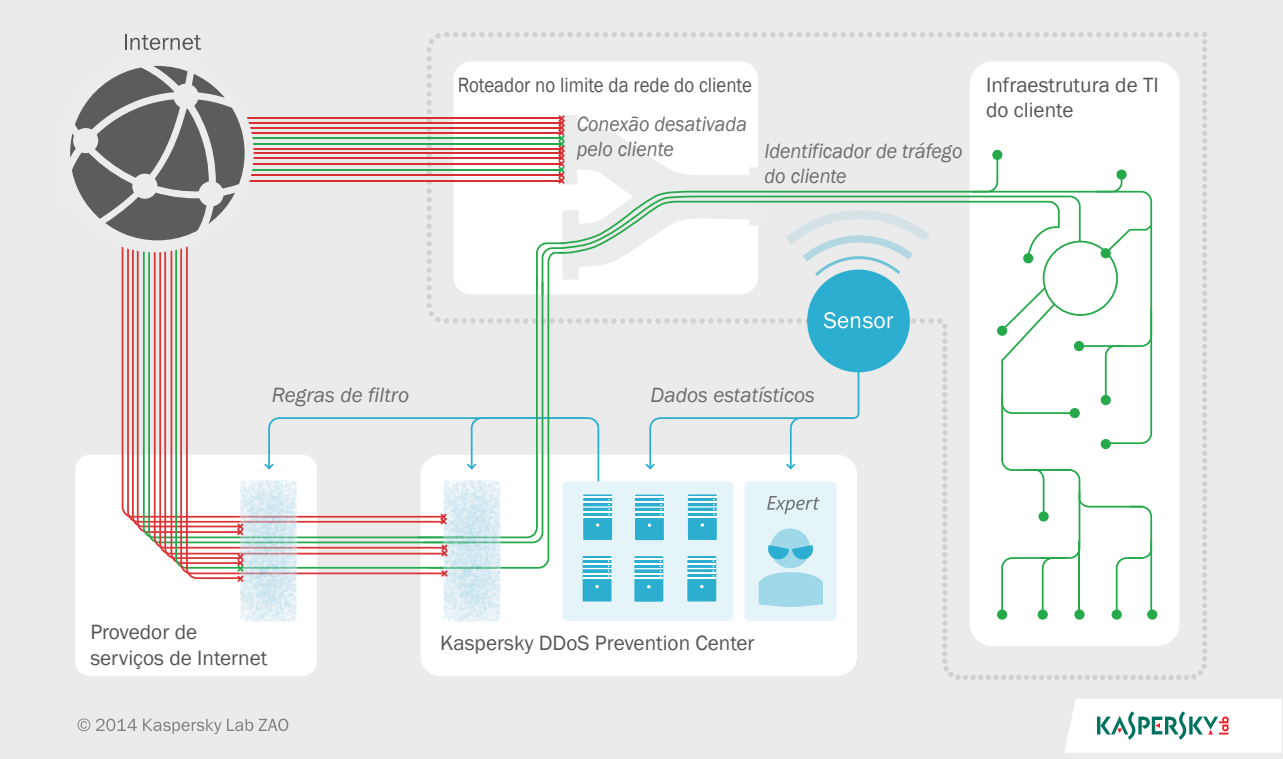

Figura 2. Kaspersky DDoS Protection: diagrama de operação

Arsenal da Kaspersky Lab

Há mais de uma década a Kaspersky Lab tem lidado com êxito com uma vasta gama de ameaças on-line. Durante esse período, os analistas da Kaspersky Lab adquiriram um nível de experiência singular, incluindo a compreensão detalhada de como os ataques DDoS funcionam. Os especialistas da empresa acompanham constantemente os desenvolvimentos mais recentes que ocorrem na Internet, analisam os métodos mais recentes para conduzir ciberataques, e melhoram as nossas ferramentas de proteção existentes. Com esse conhecimento em mãos, é possível detectar um ataque DDoS assim que ele é executado e antes que ele atinja o recurso da Web alvo.

O segundo elemento na tecnologia de proteção contra DDoS da Kaspersky é um sensor instalado próximo da infraestrutura de TI do cliente. O sensor é um software em execução no sistema operacional Ubuntu e requer um servidor x86 padrão. Ele analisa os tipos de protocolos usados, o número de bytes e pacotes de dados enviados, o comportamento do cliente no site, ou seja, os metadados ou informações sobre dados enviados. Ele não redireciona o tráfego para nenhum lugar, não o modifica nem analisa o conteúdo de mensagens. As estatísticas são entregues à infraestrutura Kaspersky DDoS Protection baseada na nuvem, na qual um perfil baseado em estatística é criado para cada cliente com base nos metadados coletados. Na verdade, esses perfis são registros de padrões de troca de informações típicas para cada cliente. Alterações nos tempos de uso típicos são registradas. Posteriormente, o tráfego é analisado; sempre que o comportamento do tráfego for diferente do perfil baseado em estatística, isso pode ser um indício de um ataque.

A chave do Kaspersky DDoS Protection está em seus centros de limpeza. Eles estão localizados nas principais linhas estruturais da Internet, em locais como Frankfurt e Amsterdã. A Kaspersky Lab utiliza simultaneamente diversos centros de limpeza, para que possa dividir ou redirecionar o tráfego que precisa ser limpo. Os centros de processamento são reunidos em uma infraestrutura de informações baseada na nuvem comum e os dados são contidos sem esses limites. Por exemplo, o tráfego da Web de clientes europeus não deixa o território europeu.

Outra forma chave de controlar o tráfego de DDoS é filtrá-lo no lado do provedor. O ISP não apenas fornece um canal de Internet, ele também pode celebrar uma parceria tecnológica com a Kaspersky Lab. Assim, o Kaspersky DDoS Protection pode eliminar o tráfego de lixo eletrônico mais óbvio, usado na maioria dos ataques DDoS, o mais próximo possível do seu ponto de origem. Isso evita os fluxos decorrentes da combinação em um único ataque poderoso e diminui a sobrecarga nos centros de limpeza, que ficam livres para lidar com o tráfego de lixo eletrônico mais sofisticado.

Ferramentas de redirecionamento de tráfego

Para que a solução de segurança funcione de forma eficaz, o primeiro requisito chave é configurar um canal de conexão entre os centros de limpeza e a infraestrutura de TI do cliente. No Kaspersky DDoS Protection, esses canais são organizados de acordo com o protocolo Generic Routing Encapsulation. Eles são usados para criar um túnel virtual entre o centro de limpeza e o equipamento de rede do cliente, através do qual o tráfego limpo é entregue ao cliente.

O redirecionamento do tráfego real pode ser feito usando um dos seguintes métodos: anunciando a sub-rede do cliente com o uso de um protocolo de roteamento dinâmico BGP, ou modificando o registro DNS por meio da introdução do URL do centro de limpeza. O primeiro método é preferível, pois ele pode redirecionar o tráfego com muito mais rapidez e proteger contra ataques que visam diretamente um endereço IP específico. No entanto, esse método necessita que o cliente tenha um intervalo de endereços que seja independente do provedor, como um bloco de endereços IP fornecido por um registrador de Internet regional.

No que diz respeito ao procedimento de redirecionamento real, há pouca diferença entre os dois métodos. Se o primeiro método for usado, os roteadores BPG no lado do cliente e no centro de limpeza estabelecem uma conexão permanente através do túnel virtual; em caso de ataque, uma nova rota do centro de limpeza para o cliente é criada. Quando o segundo método é usado, o cliente recebe um endereço IP do pool de endereços do centro de limpeza. Se um ataque começar, o cliente substitui o endereço IP no registro DNS A pelo endereço IP atribuído pelo centro de limpeza. Depois disso, todo o tráfego que chega ao endereço do cliente será enviado primeiramente para o centro de limpeza. No entanto, para impedir que o ataque no endereço IP antigo continue, o provedor precisa bloquear todo o tráfego de entrada, exceto pelos dados provenientes do centro de limpeza.

Como funciona

Em circunstâncias normais, todo o tráfego da Internet vai diretamente para o cliente. As ações de proteção começam assim que um sinal do sensor é recebido. Em alguns casos, os analistas da Kaspersky Lab sabem de um ataque assim que ele é iniciado, e informam o cliente. Nesse caso, medidas preventivas podem ser tomadas com antecedência. O especialista em DDoS disponível na Kaspersky Lab recebe um sinal de que o tráfego que chega ao cliente não corresponde ao perfil estatístico. Se o ataque for confirmado, o cliente é notificado sobre ele, e deve dar a ordem para redirecionar o tráfego para os centros de limpeza (em alguns casos, pode haver um contrato com o cliente para que o redirecionamento seja iniciado automaticamente).

Assim que as tecnologias da Kaspersky Lab determinam o tipo do ataque, regras específicas de limpeza são aplicadas para esse tipo de ataque e para o recurso da Web específico. Algumas das regras, criadas para tratar o tipo mais bruto de ataque, são comunicadas à infraestrutura do provedor e são aplicadas aos roteadores pertencentes ao provedor. O tráfego restante é entregue aos servidores do centro de limpeza e filtrado de acordo com vários sinais característicos, como endereços IP, dados geográficos, informações dos cabeçalhos HTTP, a exatidão dos protocolos e a troca de pacotes SYN etc.

O sensor continua a monitorar o tráfego conforme ele chega ao cliente. Se ele ainda mostrar sinais de um ataque DDoS, o sensor alerta o centro de limpeza, e o tráfego é submetido a uma profunda análise de comportamento e de assinatura. Com esses métodos, o tráfego malicioso pode ser filtrado com base nas assinaturas, ou seja, um tipo específico de tráfego pode ser completamente bloqueado, ou endereços IP podem ser bloqueados com base em critérios específicos observados. Dessa forma, mesmo os ataques mais sofisticados são filtrados, incluindo um ataque de sobrecarga de HTTP. Esses ataques envolvem imitações de um usuário que visita um site, mas que na verdade são caóticos, excepcionalmente rápidos e que geralmente são oriundos de um regimento de computadores zumbis.

Os especialistas da Kaspersky Lab monitoram todo o processo usando uma interface específica. Se um ataque for mais complicado do que o normal ou se ele for atípico, o especialista pode assumir o controle, alterar as regras de filtragem e reorganizar os processos. Os clientes também podem ver como a solução e o tráfego se comportam, usando sua própria interface.

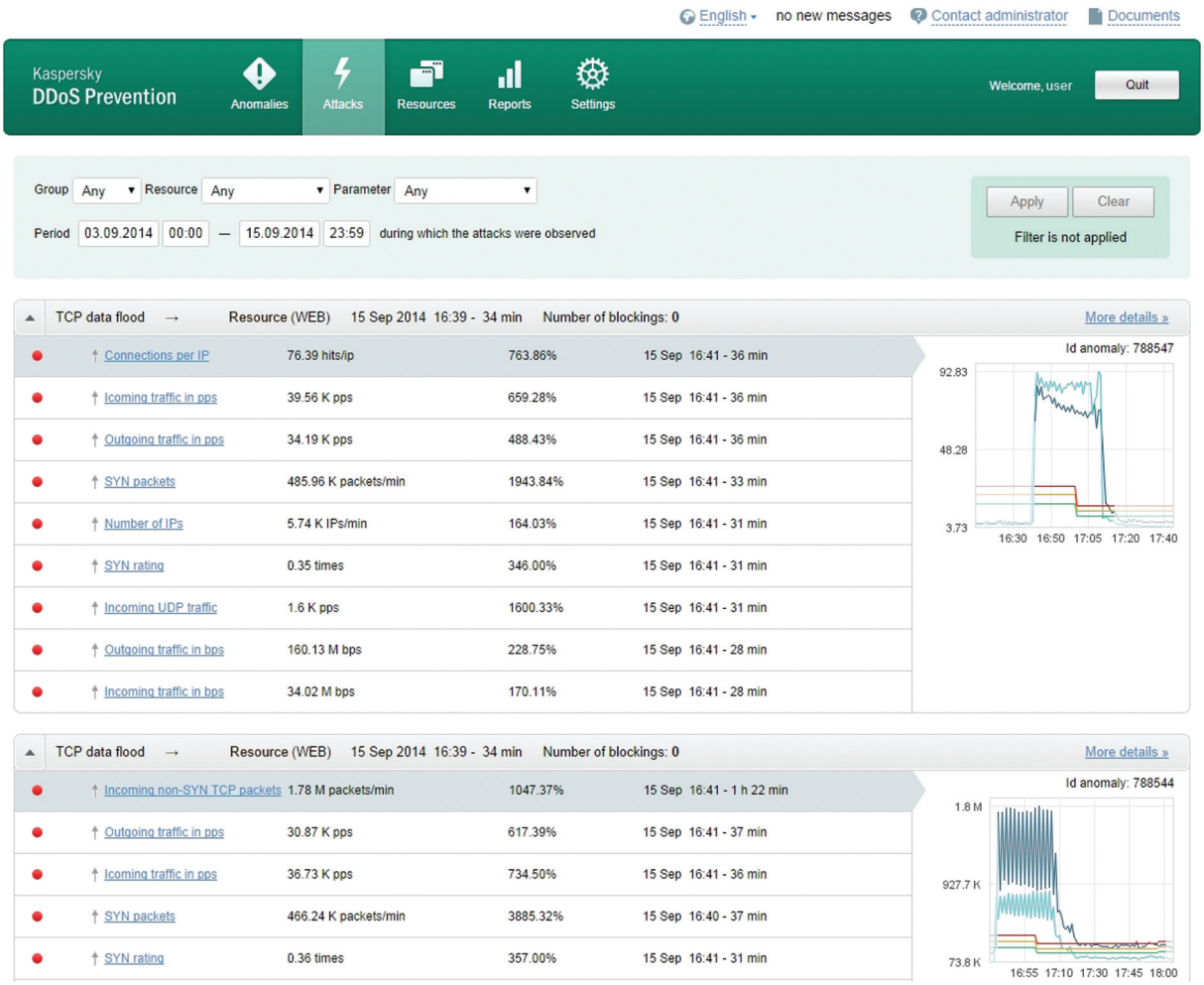

Figura 3. Captura de tela da interface do cliente

Quando o ataque tiver acabado, o tráfego é direcionado novamente aos servidores do cliente. O Kaspersky DDoS Protection é revertido para o modo de espera, e o cliente recebe um relatório detalhado do ataque, incluindo um registro detalhado de como ele se desenvolveu, gráficos representando parâmetros mensuráveis, bem como a distribuição geográfica das fontes do ataque.

Vantagens da abordagem da Kaspersky Lab

- O simples redirecionamento do tráfego para centros de limpeza da Kaspersky Lab durante um ataque e a filtragem do tráfego no lado do provedor ajudam a reduzir significativamente o custo para o cliente.
- As regras de filtragem são desenvolvidas individualmente para cada cliente, dependendo dos serviços on-line específicos que precisam ser protegidos.
- Os especialistas da Kaspersky Lab monitoram o processo e ajustam rapidamente as regras de filtragem quando necessário.
- A estreita cooperação entre os especialistas do Kaspersky DDoS Protection e os desenvolvedores da Kaspersky Lab permite adaptar a solução de forma rápida e flexível em resposta a circunstâncias volúveis.
- Para garantir o mais elevado nível de confiabilidade, a Kaspersky Lab utiliza apenas equipamentos europeus e prestadores de serviços em países europeus.
- A Kaspersky Lab acumulou uma vasta experiência na aplicação dessa tecnologia na Rússia, onde ela protege com êxito as principais instituições financeiras, agências comerciais e do governo, lojas on-line etc.

Março de 2015/Global

www.kaspersky.com