WHITE PAPER

A evolução e o aumento rápidos dos ataques DDoS

Com os ataques se tornando mais direcionados, sofisticados e frequentes, cada empresa precisa permanecer vigilante.

Nenhuma empresa passa despercebida para os ataques DDoS (negação de serviço distribuído). Os cibercriminosos, inclinados à extorsão, ao hacktivismo ou à vingança, podem facilmente atingir qualquer organização com ataques grandes e sofisticados. É por isso que cada empresa voltada para a tecnologia digital agora precisa de uma defesa holística contra ataques DDoS.

Um dos primeiros tipos de ataque da Internet

Em 22 de julho de 1999, 114 computadores comprometidos sobrecarregaram um único computador da Universidade de Minnesota com pacotes de dados supérfluos e o derrubaram, deixando-o offline por dois dias.

Segundo a MIT Technology Review, esse foi o primeiro ataque DDoS documentado.

Nas semanas e meses seguintes, grandes nomes, da CNN à Amazon, ficaram offline enquanto hacktivistas e outros cibercriminosos viram como era fácil realizar esses ataques. Eram necessárias apenas algumas linhas de código.

O DDoS se tornou uma ameaça para qualquer empresa com presença online.

Os ataques aumentam em escala e sofisticação

As defesas contra DDoS avançaram muito desde 1999. Mas os criminosos também. Os agentes de ameaças de DDoS atuais têm dezenas de vetores de ataque para utilizar e kits de ferramentas baratos para invasores, além de inúmeros dispositivos vulneráveis na Internet para amplificar suas campanhas. Em 2016, os invasores derrubaram uma grande parte da Internet usando DVRs de câmera de segurança comprometidos.

Desde então, mais centenas de milhões de dispositivos de IoT desprotegidos entraram em atividade online. A próxima revolução do 5G promete mais centenas de milhões. Imagine a força e o tamanho dos ataques impulsionados pelas melhorias exponenciais do 5G em velocidade, capacidade e latência.

O número de servidores desprotegidos e sem manutenção na Internet também está crescendo rapidamente, servidores que os criminosos podem sequestrar para ataques de amplificação e reflexão. Muitos desses servidores, e os criminosos sabem os IPs deles, podem multiplicar solicitações falsificadas por um fator de mais de 50.000.

Mitigação e proteção de emergência contra DDoS 24 horas por dia, sete dias por semana

Os clientes atuais da Akamai ameaçados por ataques DDoS devem entrar em contato com o SOCC da Akamai.

Se você não é um cliente da Akamai, mas precisa de proteção de emergência, preencha o formulário em nossa **página de linha direta de DDoS** ou ligue para o número **+1-877-425-2624** para receber assistência imediata.

Nenhum setor está imune a ataques DDoS

Hoje, a Akamai mitiga milhares de ataques DDoS todos os anos.

Em alguns casos, os motivos parecem óbvios. Um jogador pode usar ataques DDoS para reduzir a velocidade das redes e ganhar vantagem competitiva contra os rivais. Os alunos de faculdades já usaram ataques DDoS direcionados para frustrar os clientes de um ISP e direcionar os negócios para um concorrente.

Às vezes, no entanto, os motivos são mais complexos ou difíceis de entender. Temos visto criminosos usarem ataques DDoS para distrair as equipes de resposta a incidentes em uma parte de uma organização enquanto tentam um ataque menos óbvio em outra.

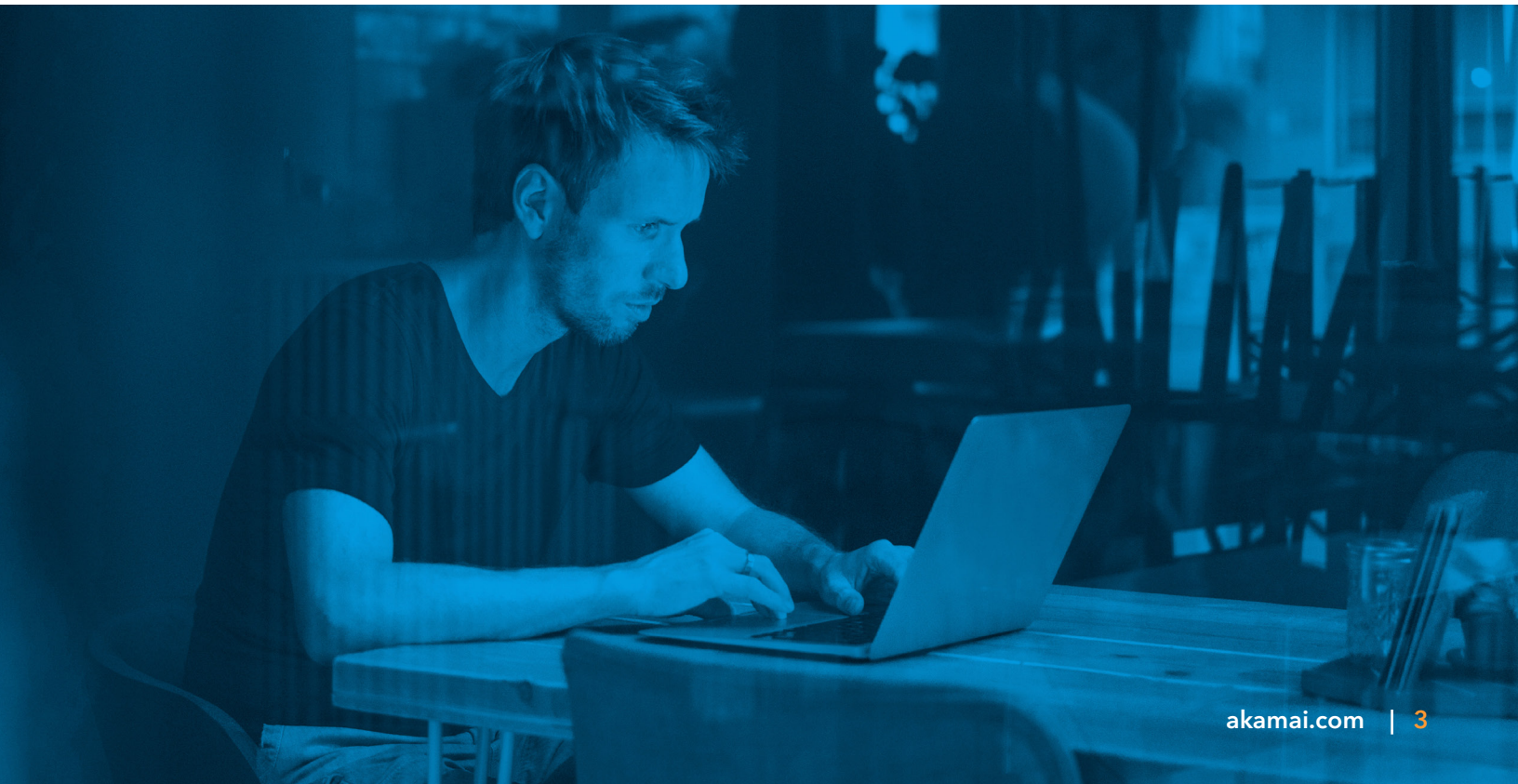
Para agentes mal-intencionados que não têm as habilidades, há negócios para a "contratação de DDoS" na darknet. Os preços começam em US$ 5 por um ataque de cinco minutos e aumentam para US$ 400 por 24 horas. Se alguém tem um problema sério, pode gastar US$ 200 ou US$ 300, e gerar um custo de milhões para uma empresa.

O ano de 2020 trouxe ataques maiores e mais sofisticados

No primeiro semestre de 2020, a Akamai interrompeu ataques maciços de 1,44 terabit por segundo (Tbps) e 809 milhões de pacotes por segundo (Mpps), o maior ataque Mpps já registrado.

Embora mitigados em menos de um segundo, esses ataques refletem uma tendência para mais ataques de 100 Gbps ou superiores. Muitos usam combinações únicas e complexas de vários vetores. Eles querem sobrecarregar ou burlar as defesas e consumir recursos de resposta a incidentes.

Os ataques que exigem pelo menos certa mitigação conduzida por humanos, e não apenas respostas automatizadas, também estão em alta.



Entre na maior campanha de extorsão de DDoS da história

Em agosto de 2020, a equipe de pesquisa de inteligência de segurança da Akamai emitiu um alerta, avisando que empresas de diversos setores receberam e-mails de extorsão de DDoS. Os invasores ameaçaram prejudicar as operações, inferindo que as empresas enfrentariam uma enorme paralisação e grandes perdas financeiras se não pagassem um resgate em Bitcoin.

Somente algumas semanas depois, o FBI relatou que milhares de organizações em todo o mundo receberam e-mails de extorsão semelhantes. Os invasores se mobilizariam e ameaçariam as empresas de um setor, depois de outro e de outro. Os invasores altamente organizados muitas vezes voltaram a ameaçar alvos anteriores.

Quanto melhor as suas defesas, menor será a probabilidade de você ser atacado

Os cibercriminosos são como qualquer criminoso. Eles monitoram o alvo, procurando por uma fraqueza. Para o DDoS, isso significa observar o DNS, as aplicações Web e os bens de data center voltados para a Internet da vítima direcionada.

Se esse reconhecimento revelar recursos, websites ou serviços vulneráveis, os cibecriminosos podem agir. Se revelar defesas reforçadas, eles geralmente partem para outra.

Na verdade, entre os novos clientes de incidentes de emergência do Prolexic que foram atacados antes do roteamento para a plataforma, a grande maioria não foi atingida novamente onde as defesas do Prolexic haviam sido implementadas. Para um cibercriminoso, os alvos defendidos pelo Prolexic podem não valer o esforço, especialmente quando há casos mais fáceis em outros lugares.

Como funciona a defesa holística contra DDoS?

A Akamai oferece defesa contra DDoS detalhada por meio de uma malha transparente de edge dedicada, DNS distribuído e soluções de mitigação de depuração na nuvem com mais de 175 Tbps de capacidade total de rede. Essas nuvens de uso específico são projetadas para fortalecer as posturas de segurança contra DDoS e, ao mesmo tempo, reduzir as superfícies de ataque. Essa proteção contra DDoS de ponta a ponta foi arquitetada para melhorar a qualidade da mitigação e reduzir falso-positivos, ao mesmo tempo em que aumenta a resiliência contra os maiores e mais complexos ataques.

Além disso, a solução pode ser ajustada aos requisitos específicos de suas aplicações Web ou serviços baseados na Internet.

Proteção da edge

A Akamai projetou sua Intelligent Edge Platform globalmente distribuída como um proxy reverso que aceita tráfego somente pelas portas 80 e 443. Todos os ataques DDoS à camada de rede são descartados instantaneamente na edge com um SLA (Acordo de Nível de Serviço) de zero segundo.

Para eventos na camada de aplicação, incluindo os iniciados por meio de APIs, o Kona Site Defender absorve os ataques e, ao mesmo tempo, concede acesso a usuários legítimos.

Proteção do DNS

O serviço de DNS autoritativo da Akamai, Edge DNS, também filtra o tráfego na edge. Diferentemente de outras soluções de DNS, a Akamai projetou o Edge DNS especificamente para oferecer disponibilidade e resiliência contra ataques DDoS. O Edge DNS também oferece desempenho superior, com redundâncias arquitetônicas em vários níveis, incluindo servidores de nomes, pontos de presença, redes e, até mesmo, nuvens IP Anycast segmentadas.

Defesa com depuração em nuvem

O Prolexic protege data centers inteiros e infraestruturas híbridas contra ataques DDoS, em todas as portas e protocolos, com 20 centros globais de depuração e mais de 8,2 Tbps de defesa dedicada contra DDoS. Essa capacidade foi criada para manter disponíveis os ativos voltados para a Internet: a base de qualquer programa de segurança da informação.

Como um serviço totalmente gerenciado, o Prolexic pode desenvolver modelos de segurança positiva e negativa. O serviço combina defesas automatizadas com mitigação especializada da rede global de SOCCs (Centros de comando de operações de segurança) da Akamai. O Prolexic também oferece um SLA de mitigação de zero segundo **líder do setor** por meio de controles defensivos proativos.

Como o Prolexic impediu um ataque que estabeleceu um recorde

O ataque de 809 Mpps de junho de 2020 foi o maior ataque de pacotes por segundo (PPS) já visto pela Internet. Diferentemente dos ataques de bits por segundo mais comuns, que tentam sobrecarregar o pipeline de Internet de entrada, os ataques de PPS têm como objetivo esgotar o mecanismo de rede no data center ou na nuvem.

Esse ataque gigantesco envolveu um enorme número de endereços IP de origem. Mais de 96% deles não haviam sido observados em ataques anteriores. O ataque também aumentou de 418 Gbps para 809 Mpps em apenas dois minutos.

Felizmente, a organização-alvo era um cliente do Prolexic, que conta com um SLA de zero segundo. O SOCC da Akamai trabalhou com esse cliente para entender seus perfis de linha de base de tráfego em tempos de tranquilidade e colocar controles e políticas de segurança em vigor para bloquear ataques DDoS instantaneamente.

Agende hoje mesmo um resumo personalizado sobre ameaças

Visite **akamai.com/ddos-briefing**