SOTI SUMMER 2018

[state of the internet] / segurança

RESUMO EXECUTIVO

Resumo executivo

A Akamai, a maior e mais confiável plataforma de entrega na nuvem do mundo, usa a Akamai Intelligent Platform™ distribuída globalmente para processar trilhões de transações pela Internet todos os dias. Isso nos permite coletar grandes quantidades de dados sobre métricas relacionadas à conectividade de banda larga, à segurança em nuvem e à entrega de mídia. Todo trimestre, a Akamai publica os relatórios *State of the Internet* com base nesses dados, concentrando-se na conectividade de banda larga e na segurança na nuvem.

IMPLICAÇÕES DE NEGÓCIOS

Os ataques que observamos nos últimos meses nos lembra que o estado da segurança na Internet nunca é estático. A ingenuidade dos invasores é continua; eles continuam a descobrindo novos vetores e exploram novas vulnerabilidades, desenvolvendo estratégias de ataque que são mais prejudiciais que nunca. Em 2017, observamos novas classes de dispositivos, como telefones móveis e dispositivos IoT, sendo usados em grandes botnets responsáveis por ataques de recorde de tamanho. No entanto, nos dois primeiros meses de 2018, esses registros anteriores já eram passado, como os invasores utilizaram um novo vetor, memcached - um serviço que, originalmente, não era pra ter sido exposto na Internet - para gerar excessivos ataques de 1 Tbps. O memcached permite que ataques sejam intensificados por ordem de magnitude maior do que qualquer outro ataque de reflexão conhecido.

Felizmente, nesse caso, uma resposta rápida dos desenvolvedores, operadores de rede e fornecedores de serviços parece ter rapidamente reduzido o número de servidores memcached vulneráveis disponíveis, com sorte, limitando o potencial deste novo vetor de ataque no futuro. Isso serve como um gentil lembrete de que a comunidade de segurança nunca pode crescer de forma complacente. Devemos estar preparados para tendências de ataque e avanços tecnológicos, além do crescimento do tamanho desses ataques. Além disso, fica por conta da comunidade, como um todo, manter-se atualizada com os patches de software e configurações seguras para minimizar os acessos criminosos a superfícies de ataque.

VISÃO GERAL DO EDITOR

Assim como o estado da segurança na Internet continua a evoluir, o mesmo acontece com este relatório. Estamos implementando mudanças na frequência, formato e estrutura das publicações, em um esforço para oferecer a você percepções de nossos dados e pesquisas do modo mais oportuno e relevante possível. A maior parte dos dados estatísticos e gráficos no DDoS e ataques a aplicativos da Web (incluindo gráficos em ataques DDoS de tamanho e frequência de vetor) foi movida para nosso site. Procure atualizações em nosso blog. Além disso, vamos publicar regularmente relatórios menores e mais simplificados que se concentram em tendências a longo prazo, pesquisas e análises. O relatório *State of the Internet / Security: Web Attack* será publicado duas vezes por ano, um a cada semestre.

Nosso evento, Summer 2018 Attack Spotlight, se concentra no ataque de reflexão memcached de fevereiro de 2018, que estabeleceu um novo recorde de maior ataque amenizado pela Akamai até o momento. Com 1,3 Tbps, o ataque mais que dobrou o registro anterior de 623 Gbps obtido por Mirai em setembro de 2016. Os ataques DDoS

1 Tbps

Limite ultrapassado pelo refletor memcached

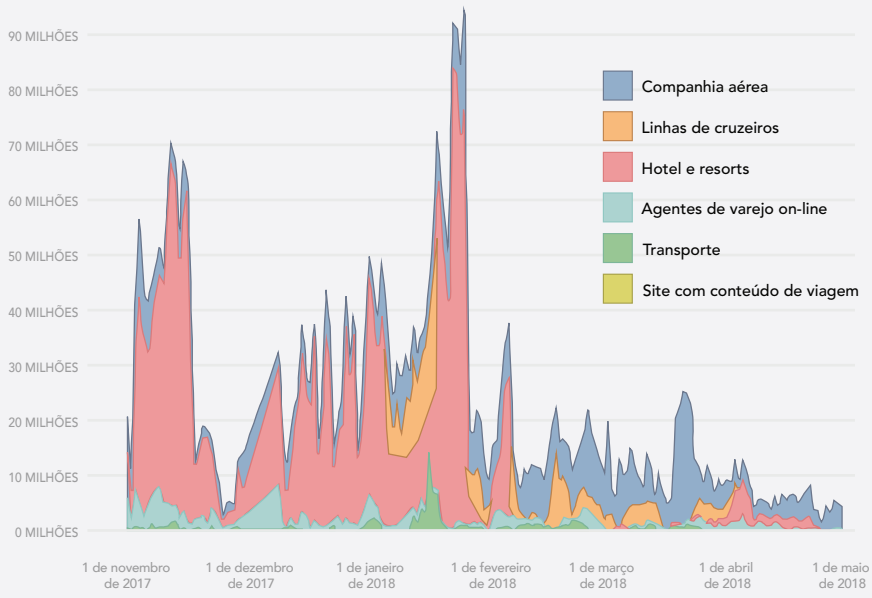
de médio porte também continuaram a aumentar ao longo do último ano, alcançando agora 1,3 Gbps, destacando a importância de cada organização na preparação para ataques de grande escala.

No relatório *Summer 2018 State of the Internet / Security: Web Attack*, examinamos alguns dos ataques DDoS que empregam táticas incomuns para aumentar a eficácia dos ataques. Embora a maioria dos ataques DDoS sejam simples e volumétricos por natureza, alguns mostram a influência de inimigos inteligentes e adaptativos que alteram as táticas para contornar as defesas em seu caminho.

Operation Power Off, um esforço das autoridades para desativar os sites de DDoS-for-hire, é um tópico de grande interesse. Um esforço coordenado em abril de 2018 entre as autoridades em vários países desativaram o site Webstresser.org, um importante participante no mercado de DDoS-for-hire, supostamente responsável por milhões de ataques. Levando em consideração o quanto esses sites são lucrativos, não nos surpreenderia se outros aparecessem para tomar seu lugar em breve.

Por fim, com base nos bots e dados de abuso de credenciais, analisamos primeiramente o relatório *Q4 2017 State of the Internet / Security*, nos aprofundamos para melhor caracterizar e entender os bots e os violadores de credenciais direcionados ao setor hoteleiro; vertical em que observamos a maior porcentagem de acessos mal-intencionados. Também observamos que o fechamento de várias rotas, no início de fevereiro de 2018, parece ter precipitado uma imensa queda no número de tráfego mal-intencionado.

fig 1.1 **Tentativas de login maliciosas: Hotel e Viagem**



ATAQUES DDOS, SEMESTRE DE 2018 VERSUS SEMESTRE DE 2017

16% de aumento no total de ataques DDoS

16% de aumento nos ataques à camada de infraestrutura (camadas 3 e 4)

4% de aumento nos ataques baseados em reflexão

38% de aumento nos ataques da camada de aplicação

Para mais análises e pesquisas, baixe o relatório completo.

O relatório *Summer 2018 State of the Internet / Security: Web Attack* reúne dados de ataques de toda a infraestrutura global da Akamai e representa a pesquisa de um conjunto diversificado de equipes em toda a empresa.

STATE OF THE INTERNET / EQUIPE DE SEGURANÇA

Jose Arteaga, Akamai SIRT, Data Wrangler — Attack Spotlight
Dave Lewis, Global Security Advocate — Operation Power Off
Wilber Mejia, Akamai SIRT — Attack Spotlight
Elad Shuster, Security Data Analyst Advanced DDoS — Akamai Blog
David McEwan, Security Operations Command Center — Advanced DDoS
Alejandro Ziegenhirt, Security Operations Command Center — Advanced DDoS

EQUIPE EDITORIAL

Martin McKeay, Gerente sênior de segurança, editor sênior
Amanda Fakhreddine, Redatora técnica sênior, editora

CRIAÇÃO

Shawn Broderick e Sajeesh Alakkaparambil, Design
Georgina Morales Hampe e Kylee McRae, Project Management

SOBRE A AKAMAI

A Akamai, desenvolvedora da principal plataforma de entrega na nuvem do mundo, possibilita que seus clientes ofereçam as melhores experiências digitais em qualquer dispositivo, a qualquer hora e em qualquer lugar. A escala da plataforma amplamente distribuída da Akamai é incomparável, com mais de 200.000 servidores em 130 países, oferecendo a seus clientes desempenho e proteção superiores contra ameaças. O portfólio de soluções de desempenho na Web e em dispositivos móveis, segurança na nuvem, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, 7 dias por semana. Para saber por que as principais instituições financeiras, os líderes de varejo on-line, os provedores de mídia e entretenimento e as organizações governamentais confiam na Akamai, acesse www.akamai.com, blogs.akamai.com ou siga @Akamai no Twitter. Nossas informações de contato globais podem ser encontradas em www.akamai.com/locations ou ligue para 877-425-2624. Publicado em 06/18.