[state of the internet] / segurança

UM ANO EM ANÁLISE

RESUMO EXECUTIVO: VOLUME 4, EDIÇÃO 5

NOTAS DO EDITOR

Desde novembro de 2017, a equipe de pesquisa da Akamai publica uma média de mais de um artigo, postagem de blog ou artigo científico por semana. Eles variam de postagens sobre eventos futuros, comunicação de crises sobre ameaças emergentes e o próprio relatório State of the Internet / Segurança. É por isso que decidimos olhar para o nosso trabalho anterior e observar como ele se encaixa no mais caso de segurança do ano passado. Com isso em mente, pedimos ao nosso Diretor de segurança, Andy Ellis, que refletisse sobre a direção à qual as tendências atuais podem nos levar em 2019. Confira a seguir um trecho de seu estudo.

ESCRITÓRIO DO CSO

> **“ plus ça change, plus c’est la même chose —**
> Jean-Baptiste Alphonse Karr

Se há uma única verdade em relação às tendências na área de segurança na Internet é que cada ano traz mais do mesmo. Em 1998, durante a Operation Desert Fox, adversários usaram um ataque distribuído de negação de serviço, que também usou a vulnerabilidade *teardrop*, na tentativa de derrubar redes da USCENTAF (eu era o engenheiro de defesa de plantão na época, por isso lembro do entusiasmo para identificar o ataque, testar uma configuração e expulsá-lo dos nossos sistemas de segurança de perímetro). Isso não é estrategicamente diferente das ações que ocorrem em nossos (e em outros) Centros de operações de segurança todos os dias, somente a escala e a automação mudaram.

Quando olhamos para 2019, é mais fácil observar padrões em andamento nos últimos anos, sugerir que eles continuarão e supor que provavelmente seguirão evoluindo, principalmente em relação ao modo como avançam.

Akamai
Experience the Edge

DDoS de força bruta

O DDoS é sempre um ótimo lugar para começar, principalmente porque as tendências de DDoS são notavelmente estáveis. Talvez seja mais fácil pensar sobre ataques em dois eixos diferentes: aproveitamento e largura de banda. A *largura de banda* é basicamente a medição do tráfego que um adversário pode gerar a qualquer momento. Historicamente, temos observado o tamanho dos maiores ataques crescer cerca de 9% por trimestre, dobrando a cada dois anos. Entretanto, o fascinante disso é que não se trata de um crescimento contínuo. Um novo pico é definido (ao longo dessa curva de QoQ de 9%) sempre que um adversário descobre uma nova maneira de construir um botnet ou reflexão, como no caso do Mirai ou de ataques de reflexão do memcached.

Entre os novos picos, dois fatos acontecem. Primeiro, as partes afetadas, como administradores de sistemas e operadores de ISP, tomam medidas para reduzir o número de sistemas disponíveis para uso em ataques. Segundo, os adversários começam a lutar pelo controle desses recursos, e observamos os botnets começarem a se fragmentar, fazendo com que ataques individuais se tornem menores.

De um ponto de vista da eficácia, isso não é de fato prejudicial ao invasor. Estilos de defesa de DDoS geralmente não são escalonados em tamanho de maneira linear. Os maiores ataques ocorrem na borda da rede, onde residem serviços como o Kona Site Defender ou o Prolexic Routed da Akamai. Defesas da camada média residem no núcleo de ISPs, fornecendo serviços "clean-pipe" para os proprietários de websites. As menores defesas, soluções no local, residem exclusivamente nos data centers de destino. Para um adversário cujo botnet não é grande o suficiente para atacar uma defesa baseada na borda, um ataque a alguém que use apenas defesas baseadas no data center ainda pode ser eficaz, mesmo com um centésimo do tamanho.

Visto que ataques DDoS baseados na largura de banda têm muitas formas, é interessante que o tamanho máximo dos ataques pareça limitado por uma curva de crescimento trimestral de 9%. Interessante, mas isso tem uma explicação. Em vez de ser causado por algum limite de ocorrência natural, a explicação mais provável é que o crescimento subjacente da Internet limita a capacidade agregada dos botnets. A capacidade da Internet atenua o peso total da carga que um ataque DDoS pode gerar; quanto maior a distância entre o destino e os componentes da rede, menor será o tráfego enfrentado em qualquer conexão congestionada entre o alvo e a origem do ataque.

Para conferir mais ideias de Andy sobre DDoS, ataques no nível da aplicação, preenchimento de credenciais, economia gig e blockchain, baixe o relatório **State of the Internet / Segurança: Um ano em análise**, Volume 4, Edição 5.

SOBRE A AKAMAI

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A plataforma de borda inteligente da Akamai cerca tudo, da empresa à nuvem, para que os clientes e seus negócios possam ser rápidos, inteligentes e protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a alcançar a vantagem competitiva por meio de soluções ágeis que estendem a potência de suas arquiteturas multinuvem. A Akamai aproxima as decisões, apps e experiências dos usuários mais do que nenhuma outra, afastando ao mesmo tempo ataques e ameaças. O portfólio de soluções de segurança de borda, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeo da Akamai conta com um excepcional atendimento ao cliente, análise e monitoramento 24 horas por dia, 7 dias por semana, durante o ano inteiro. Para saber por que as principais marcas mundiais confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou @Akamai no Twitter. Nossas informações de contato globais podem ser encontradas em www.akamai.com/locations ou ligue para 877-425-2624. Publicado em 12/18.