ATAQUES DE REFLEXÃO DO MEMCACHED:
UMA NOVA ERA PARA O DDoS

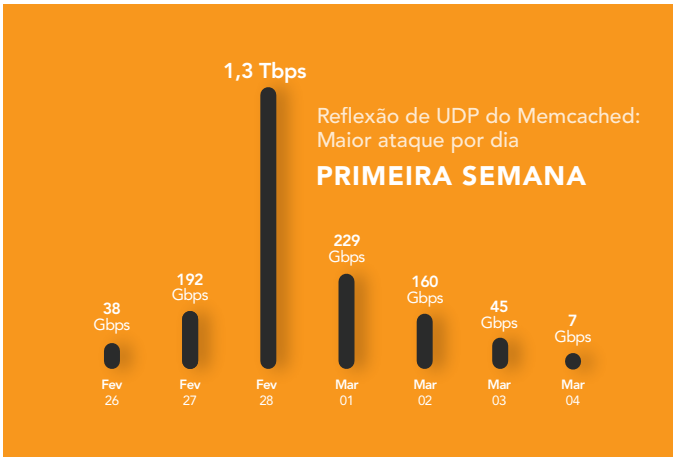
O número de ataques DDoS dobrou no início de 2018, depois que invasores descobriram e empregaram um novo método de reflexão e amplificação de DDoS com o potencial de multiplicar seus recursos de ataque por um fator de 500 K. O vetor de ataque, chamado de *reflexão de UDP do memcached*, usa recursos expostos livremente na Internet, sem a necessidade de utilizar qualquer malware ou botnet.

Em 28 de fevereiro de 2018, o maior ataque DDoS registrado até hoje foi direcionado a um cliente da Akamai, com um número recorde de 1,3 terabits por segundo (Tbps) de tráfego DDoS de reflexão do memcached. O ataque foi duas vezes maior do que o recorde anterior de ataques DDoS realizados pelos botnets Mirai de Internet das coisas (IoT).

O serviço de proteção Prolexic DDoS da Akamai atenuou esse enorme ataque DDoS imediatamente após receber o tráfego da rede do cliente, filtrando todo o tráfego proveniente da porta padrão utilizada pelo memcached, uma ferramenta de cache de dados de código-fonte aberto. O tráfego descontaminado foi devolvido à rede do cliente pelos centros de depuração de DDoS da Akamai na Europa, EUA e Ásia, sem nenhum impacto adicional nas operações do cliente.

O Memcached, normalmente utilizado para melhorar os tempos de resposta de consulta de discos e bancos de dados, foi transformado em uma arma da Internet pelos invasores que utilizam técnicas de reflexão de DDoS. O primeiro ataque DDoS atribuído à reflexão do memcached foi observado apenas dois dias antes do ataque maior. No momento do ataque de 1,3 Tbps, a Akamai já havia desenvolvido atenuações automatizadas para defender nossos clientes contra os ataques do memcached.

Durante a primeira semana, 19 ataques DDoS de reflexão do memcached foram direcionados a clientes da Akamai de diversos setores.



O impressionante fator de amplificação de 500.000 e a taxa de pacotes

A reflexão do memcached possui um fator de amplificação extraordinário: uma solicitação de 210 bytes poderia desencadear uma resposta 100 MB direcionada ao alvo. O memcached é projetado para entregar dados em alta taxa de velocidade: a taxa medida pela Akamai durante esse ataque foi de 127 milhões de pacotes por segundo (Mpps).

Em um servidor desprotegido da Internet, com o protocolo de comunicação UDP ativado por padrão, o memcached entrega seus dados a qualquer solicitação, inclusive a um endereço IP falso. Dezenas de milhares de servidores em mais de 1.000 ASNs participaram do ataque de 1,3 Tbps, e cada um entregou cerca de 1 Gbps de tráfego de ataque, em média. Pesquisadores estimam que existem mais de 90.000 servidores utilizando o memcached na Internet, dos quais mais de 50.000 estão vulneráveis a serem explorados como um refletor.

Expectativa de mais ataques DDoS do memcached e ataques DDoS por resgate

Como a comunidade de segurança tem observado com a contínua popularidade de outros vetores de DDoS de reflexão, é pouco provável que os administradores de sistema remotos consigam obter resultados imediatos para corrigir, reconfigurar ou remover servidores vulneráveis. Há uma expectativa de mais ataques DDoS do memcached no futuro.

Com os ataques DDoS de reflexão, como o memcached, os invasores não precisam de malware para infectar nem controlar bots em uma botnet. Até mesmo invasores pouco sofisticados podem iniciar um ataque. A Akamai observou um aumento nas operações de verificação para identificar servidores vulneráveis que utilizam o memcached. Um número maior de invasores se utilizará de servidores com o memcached para gerar ataques DDoS de todos os tamanhos. Além disso, cargas úteis do memcached estão sendo usadas para entregar mensagens de extorsão; a Akamai não recomenda o pagamento de qualquer resgate.

Os ataques DDoS sobrecarregam as conexões da rede local

Poucas organizações, com a exceção de um provedor de CDN (Rede de Entrega de Conteúdo) e atenuação de DDoS em nuvem bem-preparado como a Akamai e dos maiores ISPs, têm a capacidade de rede disponível para manter as operações ao enfrentar grandes ataques DDoS, e certamente não conseguem enfrentar um ataque dessa dimensão. As conexões da rede com o centro de dados e os dispositivos de roteamento de borda são os primeiros a serem sobrecarregados, impedindo a atenuação de DDoS no local.

A importância de planejar a atenuação de DDoS

O cliente da Akamai que foi atingido por este ataque DDoS recorde felizmente estava bem-preparado e, como resultado, sofreu uma queda de serviço de menos de 10 minutos antes de encaminhar seu tráfego para a Akamai para atenuação. O cliente havia contratado o serviço de proteção Prolexic DDoS antecipadamente, e tinha desenvolvido e realizado treinamentos com um manual de DDoS e, portanto, seus funcionários sabiam o que fazer e quem procurar. O tráfego de rede era monitorado e quando a anomalia foi identificada os funcionários direcionaram todo o tráfego de rede para a Akamai rapidamente, dentro de cinco minutos.

Por que a Akamai: projetada para ter resiliência contra DDoS

A Akamai protege nossos clientes contra ataques DDoS com a CDN, a rede Prolexic e a infraestrutura distribuída Fast DNS. Fazemos investimentos constantes para melhorar a resiliência dessas plataformas contra DDoS.

No que tange ao seu nível mais alto, o modelo de planejamento de recursos da Akamai considera o maior ataque que puder ser verificado e multiplica esse tráfego por um fator de escala para oferecer ampla cobertura à medida que os ataques se ampliam. Como resultado, somos capazes de atenuar com sucesso os maiores e mais sofisticados ataques DDoS, mesmo quando eles dobram de tamanho, incluindo esse ataque.

Nossa Equipe de Resiliência contra Adversários avalia continuamente novos incidentes e ameaças a fim de descobrir possíveis pontos de ruptura nos sistemas da Akamai, e trabalha junto com as equipes de engenharia para implementar atenuações automáticas e melhorar a resiliência em todas as áreas.

Resiliência contra DDoS na CDN (Rede de Entrega de Conteúdo)

Além de capacidade, projetamos nossa CDN para garantir disponibilidade e resiliência em quaisquer condições adversas, não apenas em ataques DDoS. Com mais de 220.000 servidores implantados em todo o mundo, a CDN da Akamai se ajusta de acordo com o status dos servidores individuais e encaminha automaticamente o tráfego do usuário de maneira a evitar paralisações e congestionamento. Cada servidor fornece uma defesa contra o DDoS, incluindo controles de taxa, listas negras e bloqueio geográfico.

Resiliência contra DDoS na rede Prolexic

A rede Prolexic é um dos serviços de depuração de DDoS mais eficazes do mundo. Ela é composta por sete centros de depuração globais, com mais de 3,5 Tbps de capacidade, e uma equipe de 150 profissionais de segurança que protegem contra milhares de ataques DDoS a cada mês. Cada centro de depuração tem várias conexões de operadora de camada 1, uma política pública de emparelhamento com mais de 500 parceiros e uma análise de tráfego de alto desempenho e atenuação ativa em várias camadas da pilha de OSI. Estamos sempre ampliando a capacidade de proteção contra DDoS.

Resiliência contra DDoS na infraestrutura Fast DNS

A Akamai opera com um serviço de DNS confiável, o Fast DNS, que oferece disponibilidade, velocidade e resiliência contra DDoS. Nós distribuímos os servidores de nome atribuídos aos nossos clientes em mais de 20 nuvens de DNS segmentadas para minimizar o impacto que os ataques DDoS contra qualquer cliente da Akamai possam ter sobre os demais. Os clusters de servidores de nomes e controles adicionais minimizam o impacto de ataques DDoS localizados.

Conclusão

A Akamai oferece proteção contra ataques DDoS há quase duas décadas e já protegeu nossos clientes e manteve a disponibilidade de infraestrutura até mesmo enquanto combatia os maiores ataques DDoS da época. A Akamai continua a investigar e informar sobre novas ameaças, e continuamos a desenvolver nossos procedimentos e nossa plataforma para ficar à frente daqueles mal-intencionados. Utilizamos tudo o que aprendemos defendendo nossos clientes para melhorar nossa proteção. Temos o compromisso de oferecer aos clientes da Akamai a plataforma mais robusta do setor.

Analise sua resiliência contra DDoS

Se você gostaria da ajuda da Akamai para analisar a resiliência de sua infraestrutura, entre em contato com a nossa **Organização de serviços profissionais** para marcar uma consulta com nossos Arquitetos de segurança.

Saiba mais em **https://www.akamai.com/memcached.**

Akamai