Impedindo o Avanço de Ataques DDoS

Em um mundo no qual o número de dispositivos conectados continua a crescer, novos negócios e oportunidades de crescimento estão sem dúvida surgindo em áreas como a Internet das Coisas (IoT), virtualização, comércio eletrônico e entretenimento.

No entanto, ao mesmo tempo, isso abre mais caminhos para os criminosos explorarem com ataques cibernéticos cada vez mais sofisticados. Com o aumento dos dispositivos IoT, muitos deles estão agora na forma de ataques de negação de serviço distribuído (DDoS), pelos quais uma inundação de tráfego interrompe os fluxos de tráfego normais da Internet e impede a passagem de tráfego legítimo.

Essas invasões DDoS ocorrem de várias formas, sendo comum os ataques volumétricos. Eles são projetados para consumir a largura de banda disponível, sobrecarregando a rede com tráfego e normalmente são originados por dispositivos comprometidos ou pela exploração de determinados protocolos de rede. Outro tipo são os ataques de camada de aplicação, que visam um serviço específico em um servidor, como um mecanismo de pesquisa.

A ameaça deve aumentar ainda mais à medida que a IoT se prolifera impulsionada pelo 5G e seu uso para propósitos como carros conectados - o que poderia efetivamente criar hotspots móveis a partir dos quais os ataques podem ser lançados.

Content

Tendências DDoS

Nos últimos anos assistimos a alguns ataques DDoS sem precedentes na escala de terabit. Isso foi auxiliado por métodos que surgiram como a técnica de memcached, usada no início de 2018, quando um ataque DDoS de 1,7 Tbps quebrou o recorde após a ocorrência de um ataque de 1,35 Tbps alguns dias antes.

E 2020, então, viu-se ataque DDoS ainda maior, com a Amazon Web Services relatando um evento de 2,3 Tbps que resultou em três dias de ameaça elevada e foi 44% maior doque qualquer ataque volumétricodetectado anteriormente.

NETSCOUT, por sua vez, relatou que houve um aumento de 16% na frequência de ataques DDoS globalmente no segundo semestre de 2019 com relação ao ano anterior. E embora a organização tenha notado uma queda significativa na regularidade de ataques maiores que 200 Gbps, os criminosos aumentaram o volume de atividades em menor escala enquanto usavam uma variedade sempre crescente de novos vetores de ataque ou cada vez mais vetores populares - com a NETSCOUT destacando que foram sete somente em 2019.

A COVID-19 também mostrou evidências do potencial impacto de eventos repentinos que transformam o comportamento do consumidor. A empresa de serviços de informação e tecnologia Neustar destaca que no primeiro semestre de 2020, um aumento “vertiginoso” na atividade de DDoS refletiu no crescimento no tráfego da Internet, já que as pessoas passaram muito mais tempo online em casa em atividades como fazer compras, jogar e trabalhar durante a pandemia. Ao todo, a Neustar observou um aumento de 150% na quantidade de ataques nos primeiros seis meses de 2020 com relação ao ano anterior.

Uma tendência recente tem sido o aumento de ataques DDoS na área de jogos, onde se tornou mais fácil e muito mais acessível para usuários regulares armados com um cartão de crédito acessar serviços baratos que causam um atraso nas conexões dos rivais. Os serviços de “booter” ou “stresser” de DDoS de baixo custo podem ser usados para derrubar outros jogadores ou lançar ataques contra alvos como serviços financeiros, serviços regulares de TI ou de nuvem que podem hospedar aplicações para outros setores.

Outro fator a considerar é que essas ameaças podem afetar uma ampla variedade de setores, o que significa que as empresas simplesmente não podem baixar a guarda.

> “ Uma tendência recente tem sido o **aumento de ataques DDoS** na área de jogos ... Os serviços de **“booter”** ou **“stresser”** de DDoS podem ser usados para derrubar outros jogadores...

> “A mitigação automática com provedores como a NTT pode permitir uma resposta rápida em menos de **30 segundos.**

Estratégia de Combate

Para lutar contra essas ameaças, há uma variedade de passos que as operadoras e empresas podem seguir para se prepararem. Uma das principais medidas é identificar ativos que são essenciais para os negócios, como name e base servers.

Além disso, é aconselhável aproveitar os centros de operações de rede (NOCs) para ficar de olho em quais são os níveis normais de tráfego para que o impacto de um ataque possa ser mais fácil e rapidamente identificado antes que ele tenha a chance de assumir e causar um verdadeiro caos. Muitas empresas ainda não conhecem quais são seus padrões normais, o que dificulta a identificação de níveis atípicos de atividade.

Ferramentas como o NetFlow podem ser usadas para coletar dados e tráfego de rede para análise, com a grande vantagem do software poder ser comercial e open-source para caber em todos os orçamentos.

Esses recursos permitem acumular dados históricos e ajudam a identificar, no futuro, se há algum grande pico de tráfego que possa indicar um ataque - e até mesmo de onde ele pode estar vindo.

Também vale a pena manter logs detalhados de quaisquer ataques para ajudar a se preparar adequadamente para eventos semelhantes no futuro, permitindo a criação de uma lista de verificação e auxiliando uma revisão dos serviços de segurança potenciais que podem lidar com os tipos de padrão sinalizados.

Simulações de ataque podem adicionalmente ser executadas para garantir que os NOCs sejam capazes de lidar com ameaças e tenham um plano de ação específico quando elas ocorrerem, ajudando a identificar ativos críticos antes que os negócios sejam atacados. A Equipe de Segurança de Rede (NST) da divisão Rede IP Global da NTT está disposta a participar desses “jogos de guerra”, portanto, incentiva ativamente os clientes a contactar a empresa se quiserem configurá-los. Além disso, estabelecer um relacionamento próximo com as equipes de segurança dos provedores é uma forma eficaz de ajudar a aliviar o estresse quando ocorre um ataque.

Seguindo esses passos, uma resposta ao ataque pode ser dada mais rapidamente em colaboração com um provedor de rede como a NTT.

As equipes podem, então, trabalhar juntas de forma eficaz para eliminar quaisquer ameaças, usando métodos como bloqueio do tráfego ou depuração e limpeza, dependendo da necessidade. A mitigação automática com provedores como a NTT pode permitir uma resposta rápida em menos de 30 segundos – o que é importante considerando o número crescente dos ataques curtos em áreas como jogos, que geralmente duram menos de cinco minutos.

Revise e Colabore

O trabalho não deve parar depois que um ataque termina: então é hora de uma autópsia, analisando o que aconteceu e identificando quaisquer falhas de equipamento e lacunas que possa haver nas defesas para estar ainda mais pronto para ataques da próxima vez.

Dessa forma, fatores podem ser avaliados, como se os firewalls foram capazes de lidar com tráfego ruim, se havia servidores comprometidos ou vulneráveis e se há necessidade de fazer atualizações ou usar um serviço de mitigação mais inteligente.

Documentar o tipo de ataque pode ajudar as equipes do NOC a identificar tipos de tráfego maliciosos no futuro, permitindo uma resposta mais rápida. Após um ataque, também pode ser possível rastrear um ataque até o invasor e, como resultado, tomar medidas contra ele.

Além disso, a colaboração do setor é fundamental para reduzir o impacto das ameaças: o Fórum de Líderes Globais busca reunir operadoras e pessoas que lidam com DDoS regularmente para compartilhar idéias e informações, bem como ajudar as pessoas a se conhecerem para formar pontos de contato rápidos; e grupos de segurança online como NSP-SEC e Ops-Trust são outras vias de cooperação.

A NTT DATA colabora através de muitos grupos e eventos, portanto, está pronta para organizar reuniões para discutir melhores abordagens para mitigar ataques DDoS.

Proteção DDoS com a NTT DATA

Tornar a proteção uma característica central ao lançar novos produtos e serviços continua sendo uma necessidade - e é uma área onde aNTT adota uma abordagem proativa. Isso significa que as ameaças podem ser interrompidas antecipadamente, em vez de adotar uma abordagem reativa quando o dano já estiver feito.

Com essa visão, os Serviços de Proteção DDoS (DPS) oferecidos pela divisão Rede IP Global da NTT fornecem recursos inteligentes de mitigação DDoS que limpam o tráfego malicioso antes que ele afete a conexão de Internet do cliente. Isso acontece com o tráfego sendo desviado para os centros de depuração da empresa, onde é analisado e o tráfego de ataque removido antes de ser encaminhado para a rede do cliente.

A NTT, entretanto, desenvolveu vários níveis de DPS que atendem aos diferentes tipos de proteção que os clientes da Rede IP Global exigem.

O serviço DPS Max da empresa é voltado para clientes que desejam proteção total, incluindo detecção de ataques e funções de mitigação automática. Este último recurso permite que os clientes recebam mitigação imediata por meio da plataforma, detectando ataques e automaticamente implementando medidas defensivas baseadas nos limiares definidos pelo cliente. Depois que um ataque termina, a plataforma retorna o tráfego do cliente para o roteamento padrão pré-ataque.

Outras camadas de serviço da NTT são DPS Control, DPS Core e DPS Detect. O primeiro deles é um serviço de nível básico que permite aos clientes definir listas de controle de acesso (ACLs) permanentes para bloquear determinados tipos de tráfego na rede. Os tipos ideais de cliente para este serviço são usuários avançados que entendem seu perfil de tráfego e têm a capacidade de amplamente mitigar os ataques por conta própria, mas desejam reduzir sua exposição a tipos específicos de ameaça.

A camada intermediária, o DPS Core, leva as coisas para o próximo nível, oferecendo uma gama de recursos extras em comparação com o serviço básico. Um destaque desse serviço é o uso de tecnologia de ponta que possibilita respostas rápidas às solicitações de mitigação. Elepermite uma resposta em 15 minutos para solicitações enviadas por meiodo Portal DPS da empresa, um portal exclusivo para serviços de proteção DDoS.

O Portal DPS oferece grandes benefícios para os clientes, além de aumentar a rapidez. Ao abrir tíquetes na estrutura de suporte da NTT, o Portal notifica imediatamente um engenheiro de segurança de plantão para vir em auxílio do cliente. Por meio do portal, os clientes também podem solicitar mudanças de configuração, como adicionar prefixos para proteção e revisar o histórico de atenuação e gráficos de ataques.

A outra camada do serviço é o DPS Detect, que fornece os recursos oferecidos pelo DPS Core e adiciona serviços, como recursos de detecção para notificar os clientes sobre ataques potenciais e mitigação iniciada pelo cliente com o toque de um botão.

A NTT também oferece a seus clientes da Rede IP Global o blackholing seletivo para bloquear o tráfego na rede e limitar ataques baseado na geografia. Isso pode ser eficaz na prevenção da propagação de ataques volumétricos em grande escala.

Garantia extra

Uma camada adicional de garantia é fornecida pelosuporte da Equipe de Segurança de Rede IP Global, por meio do qual os assinantes dos serviços DPS podem receber acesso direto a especialistas com uma média de mais de 10 anos de experiênica, oferecendo uma vasta experiência para ajudar a mitigar ataques.

Os serviços DPS da Rede IP Global são ideais paraqualquer negócio que exija um alto nível dedisponibilidade de internet, incluindo e-commerce, operadoras de telecomunicações, provedores de serviços de internet, provedores de conteúdo, como empresas de vídeo e jogos, e sites de rede social.

De modo geral, uma abordagem multiestratégia é frequentemente recomendada pelos fornecedores como a melhor e mais abrangente estratégia para lidar com ataques DDoS atualmente. Isso emprega uma combinação de filtragem no front end para bloquear aplicações não usadas, blackholing seletivo e mitigação DDoS por meio de depuração inteligente.

Seguindo as etapas recomendadas acima e trabalhando em estreita colaboração com a NTT e seus mecanismos bem estabelecidos de segurança, grandes avanços podem ser feitos na resolução conjunta de problemas de DDoS.

> “ Os Serviços de Proteção DDoS (DPS) oferecidos pela divisão Rede IP Global da NTT fornecem recursos inteligentes de mitigação de DDoS que **limpam o tráfego malicioso antes que ele afete** a conexão de Internet do cliente.

Para mais informações ou feedback, entre em contato conosco:

gin@ntt.net

