Preparação e resposta a ataques de negação de serviço

Publicado pela primeira vez: setembro de 2011
Última atualização: março de 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

Introdução

Esta publicação foi desenvolvida pela Australian Signals Directorate (ASD) (Agência responsável por sinais de inteligência) em cooperação com o Centro Nacional de Segurança Cibernética da Nova Zelândia (NCSC-NZ), a Akamai Technologies Ltd e a Cloudflare Pty Ltd, em resposta a uma tendência crescente de ataques de negação de serviço (DoS) na nossa região. Oferece orientações às organizações sobre as melhores práticas de mitigação com base nas técnicas de ameaças contemporâneas, para se prepararem e responderem a ataques DoS.

Recomendamos que leia este conselho juntamente com as publicações da ASD *Dispositivos da Internet das Coisas* e *Proteja o seu Wi-Fi e roteador*. Estas publicações ajudam os indivíduos a evitar contribuir involuntariamente para ataques DoS que podem afetar outras pessoas.

Os ataques DoS são ataques cibernéticos destinados a interromper ou degradar serviços online, tais como websites, e-mail e serviços de Sistema de Nomes de Domínio (DNS), para negar o acesso a utilizadores legítimos. Isto é geralmente conseguido inundando um serviço online com dados, ligações ou pedidos para sobrecarregar o serviço e degradar a sua funcionalidade.

Os ataques DoS normalmente requerem uma grande quantidade de tráfego de rede para serem bem-sucedidos. Estão a tornar-se cada vez mais comuns, em parte devido ao aumento do número de dispositivos da Internet das Coisas (IoT) facilmente comprometidos. Como os fabricantes de IoT muitas vezes priorizam a experiência do utilizador em detrimento da segurança cibernética, os dispositivos vulneráveis podem incluir artigos domésticos comuns que se conectam à Internet, como TVs inteligentes, cafeteiras, aspiradores e sistemas de segurança. Esses dispositivos podem frequentemente ser comprometidos remotamente por agentes maliciosos para criar uma 'botnet' de dispositivos através da qual geram esse tráfego de rede, o que pode resultar em residências e organizações a contribuírem involuntariamente para a infraestrutura que permite a ocorrência de ataques DoS.

Atividades recentes indicam que, depois de comprometerem um grande número de dispositivos IoT, eles podem alugar ou vender essa infraestrutura a cibercriminosos e hacktivistas, que estão cada vez mais interessados em realizar ataques DoS contra alvos da sua escolha. Na maioria dos casos, os ataques DoS são realizados para causar perdas de produtividade e financeiras a uma organização, ou para chamar a atenção do público para uma causa. Um exemplo dessa atividade é descrito no aviso da ASD *Atores ligados à República Popular da China comprometem roteadores e dispositivos IoT para operações de botnet*.

À medida que a nossa economia se torna cada vez mais digitalizada e o número de dispositivos IoT mal protegidos conectados à Internet cresce, é provável que os ataques DoS continuem a aumentar.

A fim de interromper ou degradar os serviços online de uma organização, os agentes maliciosos utilizam várias abordagens, incluindo:

- direcionar um grande volume de tráfego de rede indesejado para serviços online, numa tentativa de consumir toda a largura de banda disponível da rede
- direcionar tráfego de rede personalizado para serviços online, numa tentativa de consumir os recursos de processamento dos seus computadores
- utilizar vários computadores, dispositivos IoT ou outros dispositivos ligados à Internet para direcionar o tráfego de rede para serviços online a partir de múltiplas direções e em escala muito maior, um tipo comum de ataque DoS conhecido como ataque DoS distribuído (DDoS)
- sequestrar o registo de domínio ou os servidores DNS de uma organização, numa tentativa de redirecionar utilizadores legítimos para longe dos serviços online da organização.

As organizações não podem evitar ser alvo de ataques DoS, mas existem uma série de medidas que elas podem implementar para se prepararem e, potencialmente, reduzirem o seu impacto. Preparar-se para ataques DoS antes que eles ocorram é a melhor estratégia, porque sem preparação, é difícil e menos eficaz responder durante um ataque DoS.

Embora as organizações se concentrem principalmente em proteger-se contra ataques DoS, elas também devem tomar medidas para impedir que os seus serviços online e dispositivos conectados à Internet sejam usados por pessoas com más intenções pum nível de proteção mais elevadoas.

Preparação para ataques DoS

No contexto de um volume crescente de ataques DoS em toda a nossa região, antes de implementar quaisquer medidas para se preparar para ataques DoS, a sua organização deve primeiro avaliar os seus requisitos comerciais para determinar se cada um dos seus serviços online deve permanecer operacional durante ataques DoS ou se interrupções temporárias do serviço são aceitáveis.

Se a sua organização quer aumentar a sua capacidade de resistir a ataques DoS, deve implementar proativamente as seguintes medidas, quando apropriado e prático, antes que os ataques DoS ocorram.

- Se a sua organização estiver a utilizar uma rede de entrega de conteúdos (CDN), deve implementar as seguintes medidas adicionais, quando apropriado e prático.
  - Considere utilizar uma CDN que inclua funcionalidades para proteger o seu servidor web de origem contra uma variedade de ataques à camada de aplicação e rede – algumas CDNs podem incluir essas funcionalidades como parte de uma firewall de aplicações web na periferia.
  - Evite a divulgação pública desnecessária do endereço IP (Internet Protocol) do seu servidor web de origem e certifique-se de que qualquer exposição pública esteja protegida contra ataques DoS.
  - Evite utilizar um endereço IP para o seu servidor web de origem que possa ser previsto por agentes maliciosos, por exemplo, um endereço IP na mesma sub-rede de endereços IP divulgados publicamente dos seus serviços online.
  - Use controlos de acesso à rede (como uma firewall) para garantir que apenas a CDN e as redes de gestão autorizadas da sua organização possam aceder ao seu servidor web de origem.
  - Considere utilizar uma conectividade de rede diversificada e resiliente, que pode incluir conectividade de rede privada, entre o seu servidor web de origem e o seu fornecedor de CDN, se necessitar de um nível de proteção mais elevado para o seu servidor web de origem.
  - Configure o CDN, o servidor web de origem e os cabeçalhos HTTP do cliente para otimizar a quantidade de cache realizada.
  - Considere particionar os servidores web de origem de maneira que as solicitações de endereços IP de menor risco sejam tratadas separadamente das solicitações de endereços IP de maior risco, se você precisar de um nível mais alto de disponibilidade.

- Determine quais funcionalidades e qualidades de serviço são aceitáveis para os utilizadores legítimos dos seus serviços online, como manter essa funcionalidade e quais outras funcionalidades não são necessárias durante ataques DoS.
- Adquira e utilize um serviço de mitigação de ataques DoS baseado na nuvem.
- Considere reduzir a superfície de ataque da sua organização através das seguintes medidas:
  - terceirizar serviços online fundamentais (como DNS) a prestadores de serviços conceituados que sejam capazes de resistir a ataques DoS
  - separar serviços online críticos (como o e-mail) de outros serviços online que são mais suscetíveis a serem alvo de ataques (como os sites)
  - garantir que o serviço de mitigação de ataques DoS permita apenas o tráfego de rede associado às portas de rede do serviço online.
- Discuta com os seus fornecedores de serviços os detalhes das suas estratégias de prevenção e mitigação de ataques DoS, especificamente as suas:
  - capacidade comprovada de resistir a ataques DoS em todo o mundo
  - história comprovada de tratamento de ataques DoS e testes abrangentes de ataques DoS autorizados
  - capacidade de mitigar automaticamente a maioria dos tipos de ataques DoS sem intervenção humana, como a análise manual do tráfego de rede
  - abordagem para definir os preços dos seus serviços, como se o custo é fixo ou varia consoante a quantidade de tráfego de rede e recursos de processamento do computador utilizados, e se é possível definir um limite de faturação
  - limites para notificá-lo ou desativar os seus serviços online durante ataques DoS
  - ações pré-aprovadas que podem ser realizadas durante ataques DoS
  - Acordos de prevenção de ataques DoS com fornecedores a montante.
- Implementar medidas para detetar ataques DoS, tais como monitorização em tempo real e alertas sobre a disponibilidade do sistema, tráfego de rede, recursos de processamento do computador e custos associados.
- Prepare uma versão estática do seu site que exija o mínimo de processamento e largura de banda para facilitar a continuidade do serviço durante ataques DoS.
- Adquira e utilize serviços online altamente resilientes com elevada largura de banda, recursos de processamento informático adequados, locais de alojamento geograficamente dispersos e limpeza de tráfego baseada na nuvem para descartar tráfego de rede indesejável – isto geralmente inclui a utilização de uma CDN de renome para armazenar em cache o conteúdo estático do site e proteger o seu servidor web de origem contra tráfego de rede indesejado.
- Proteja os nomes de domínio da sua organização utilizando o bloqueio de registador, confirmando se os detalhes de contacto do registo de domínio e outros detalhes estão corretos e siga as orientações adicionais descritas na publicação *Segurança do Sistema de Nomes de Domínio para proprietários de domínios* da ASD.
- Mantenha atualizados os dados de contacto dos seus prestadores de serviços e partilhe os dados de contacto da sua organização com eles, assegurando que todos os contactos estejam disponíveis consoante os requisitos da sua organização, por exemplo, 24 horas por dia, 7 dias por semana.
- Forneça os detalhes de contacto fora da banda da sua organização a um canal de comunicação fiável para os seus prestadores de serviços, para quando os canais de comunicação normais falharem.
- Desenvolva, implemente e mantenha um plano de resposta a incidentes de segurança cibernética, cobrindo vários tipos de ataques DoS contra cada um dos seus serviços online necessários para resistir a ataques DoS, e execute o plano pelo menos uma vez por ano.

- Desenvolva aplicações para proteger funcionalidades comumente abusadas que consomem mais recursos de processamento informático ou que acarretam custos financeiros adicionais (como o envio de mensagens SMS).
  - As proteções incluem limitação de taxa e verificação de que as solicitações são feitas por seres humanos.
  - Realize testes de ataque DoS, incluindo a visar fluxos lógicos inadequados na funcionalidade da aplicação.
  - Realize testes de carga mais amplos para identificar e corrigir vetores DoS.

Respondendo a ataques DoS

Se a sua organização não estiver preparada para ataques DoS, pode tentar implementar algumas das medidas acima durante os ataques DoS, embora elas possam ser menos eficazes e demorar a implementar, reduzindo a capacidade de resposta da sua organização.

A sua organização deve implementar as seguintes medidas durante ataques DoS, quando apropriado e prático.

- Execute o seu plano de resposta a incidentes de segurança cibernética.
- Pergunte aos seus prestadores de serviços se eles são capazes de implementar ações responsivas imediatamente – se ainda não tiver discutido a sua capacidade de resposta, poderá descobrir que eles são incapazes ou não estão dispostos a responder, ou cobram taxas adicionais.
- Desative funcionalidades não essenciais ou remova conteúdos não essenciais dos seus serviços online que tornam o ataque DoS atual eficaz, por exemplo, implemente uma versão do seu site sem funcionalidade de pesquisa, conteúdo dinâmico ou ficheiros grandes.
- Mantenha a comunicação com os seus clientes e prestadores de serviços, incluindo o seu prestador de serviços de mitigação de ataques DoS, e continue a monitorizar a disponibilidade dos seus serviços online.
- Considere alterar o endereço IP do seu servidor web de origem se este estiver a ser diretamente alvo e evite divulgar publicamente o novo endereço IP sem ter proteções em vigor.
- Comunique o ataque DoS às partes interessadas, incluindo a ASD e a NCSC-NZ, conforme indicado na secção 'Detalhes de contacto' desta publicação.

Evite contribuir para ataques DoS

A sua organização deve implementar as seguintes medidas para evitar contribuir involuntariamente para ataques DoS que possam afetar outras pessoas.

- Evite expor à Internet serviços, dispositivos IoT e outros dispositivos ligados à Internet que sejam desnecessários, configurados de forma insegura ou mantidos de forma inadequada.
- Configure, mantenha e monitorize com segurança os serviços, dispositivos IoT e outros dispositivos ligados à Internet que estão expostos à Internet.
  - Orientações adicionais para pequenas empresas estão disponíveis nas publicações da ASD *Dispositivos da Internet das Coisas* e *Proteja o seu Wi-Fi e roteador*.

Se a sua organização estiver a operar serviços online, deve implementar as seguintes medidas adicionais.

- Priorize a revisão dos protocolos descritos nas recomendações da Agência de Segurança Cibernética e Infraestrutura dos Estados Unidos (CISA) *sobre ataques de amplificação baseados em UDP*.
- Monitorize novos vetores de amplificação à medida que forem identificados e proteja os seus serviços online contra eles.
- Configure os controlos de acesso à rede tanto de entrada como de saída para limitar o acesso a serviços e organizações online autorizados.
- Bloqueie o acesso público anónimo a serviços online propensos a amplificação, caso não sejam necessários.
- Considere implementar um mecanismo de limitação de taxa para reduzir as consequências do abuso, se bloquear ou aplicar controlos de acesso não for possível ou apropriado.

Informação adicional

O Manual de Segurança da Informação da ASD é uma estrutura de segurança cibernética à qual as organizações podem recorrer para proteger os seus sistemas e dados contra ameaças cibernéticas. As recomendações contidas em *Estratégias para mitigar incidentes de segurança cibernética*, juntamente com Oito princípios essenciais, complementam esta estrutura.

O *Manual de Segurança da Informação da Nova Zelândia* é o manual do Governo da Nova Zelândia sobre garantia da informação e segurança dos sistemas de informação. É um manual prático concebido para satisfazer as necessidades dos responsáveis pela segurança da informação das agências, bem como dos fornecedores, contratantes e consultores que prestam serviços às agências.

Mais informação sobre vários tipos de ataques DoS está disponível nas publicações de CISA *Guia Rápido DDoS* e *Compreendendo e respondendo a publicações de ataques distribuídos de negação de serviço*.

Detalhes de contacto

Na Austrália, se tiver alguma dúvida sobre esta orientação escreva para a ASD ou ligie para 1300 CYBER1 (1300 292 371).

Na Nova Zelândia, para relatar um incidente de segurança cibernética, envie um e-mail para incidents@ncsc.govt.nz ou acesse a de NCSC-NZ Relatar um incidente.

Isenção de responsabilidade

O conteúdo deste guia é de natureza geral e não deve ser considerado como aconselhamento jurídico, nem utilizado como referência em circunstâncias específicas ou situações de emergência. Em qualquer assunto importante, deve procurar o aconselhamento profissional independente adequado em relação às suas circunstâncias pessoais.

A Commonwealth não se responsabiliza por quaisquer danos, perdas ou despesas incorridos como resultado da confiança nas informações contidas neste guia.

Para mais informação ou para relatar um incidente de segurança cibernética, contacte-nos:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Este número está disponível para uso apenas dentro da Austrália.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre