Preparing for and responding to denial-of-service attacks

First published: September 2011
Last updated: March 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

Introduction

This publication was developed by the Australian Signals Directorate (ASD) in cooperation with New Zealand's National Cyber Security Centre (NCSC-NZ), Akamai Technologies Ltd and Cloudflare Pty Ltd, in response to an increased trend in denial-of-service (DoS) attacks in our region. It offers guidance to organisations on best practice mitigations based on contemporary threat tradecraft, to prepare for and respond to DoS attacks.

We recommend reading this advice in conjunction with ASD's *Internet of Things devices* and *Secure your Wi-Fi and router* publications. These publications help individuals to avoid unintentionally contributing to DoS attacks that could impact others.

DoS attacks are cyberattacks designed to disrupt or degrade online services such as websites, email and Domain Name System (DNS) services, to deny access to legitimate users. This is typically achieved by flooding an online service with data, connections or requests to overwhelm the service and degrade its functionality.

DoS attacks typically require a large amount of network traffic to be successful. They are becoming increasingly common, in part due to an increase in the number of easily compromised Internet of Things (IoT) devices. As IoT manufacturers often prioritise user experience over cybersecurity, vulnerable devices can include regular household items that connect to the internet such as smart TVs, kettles, vacuum cleaners and security systems. These devices can often be remotely compromised by malicious actors to create a 'botnet' of devices from which to generate this network traffic, which can result in households and organisations unintentionally contributing to the infrastructure that allows DoS attacks to occur.

Recent activity indicates that once malicious actors have compromised a large number of IoT devices, they may rent or sell this infrastructure to cybercriminals and hacktivists, who are increasingly interested in performing DoS attacks against targets of their choosing. In most cases, DoS attacks are performed to cause an organisation productivity and financial loss, or to gain public attention for a cause. An example of this activity is described in ASD's *People's Republic of China-linked actors compromise routers and IoT devices for botnet operations* advisory.

As our economy further digitises and the number of poorly secured IoT devices connected to the internet grows, DoS attacks are likely to continue to increase.

To disrupt or degrade an organisation's online services, malicious actors use a number of approaches, including:

- directing a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth
- directing tailored network traffic at online services in an attempt to consume their computer processing resources
- using multiple computers, IoT devices or other internet-connected devices to direct network traffic at online services from multiple directions and on a much larger scale, a common type of DoS attack referred to as a distributed DoS (DDoS) attack
- hijacking an organisation's domain registration or DNS servers in an attempt to redirect legitimate users away from the organisation's online services.

Organisations cannot avoid being targeted by DoS attacks, but there are a number of measures that organisations can implement to prepare for and potentially reduce their impact. Preparing for DoS attacks before they occur is the best strategy, because without preparation, it is difficult and less effective to respond during a DoS attack.

Although organisations primarily focus on protecting themselves from DoS attacks, they should also take steps to prevent their online services and internet-connected devices from being abused by malicious actors to target others.

Preparing for DoS attacks

In the context of an increasing volume of DoS attacks across our region, before implementing any measures to prepare for DoS attacks, your organisation should first assess its business requirements to determine if each of your online services must remain operational during DoS attacks, or if temporary service interruptions are acceptable.

If your organisation wants to increase its ability to withstand DoS attacks, you should proactively implement the following measures, where appropriate and practical, prior to DoS attacks occurring.

- If your organisation is using a content delivery network (CDN), you should implement the following additional measures, where appropriate and practical.
  - Consider using a CDN that includes functionality to protect your origin web server from a variety of application and network layer attacks – some CDNs might include these features as part of a web application firewall at the edge.
  - Avoid unnecessary public disclosure of your origin web server's Internet Protocol (IP) address, and ensure that any public exposures are protected from DoS attacks.
  - Avoid using an IP address for your origin web server which malicious actors could predict, for example, an IP address in the same network subnet of publicly disclosed IP addresses of your online services.
  - Use network access controls (such as a firewall) to ensure that only the CDN and your organisation's authorised management networks can access your origin web server.
  - Consider using resilient diverse network connectivity, which might include private network connectivity, between your origin web server and your CDN provider, if you require a higher level of protection for your origin web server.
  - Configure the CDN, origin web server and client HTTP headers to optimise the amount of caching performed.
  - Consider partitioning origin web servers so that requests from lower risk IP addresses are handled separately to requests from higher risk IP addresses, if you require a higher level of availability.

- Determine what functionality and quality of service is acceptable for legitimate users of your online services, how to maintain that functionality, and what functionality is not required during DoS attacks.
- Procure and use a cloud-based DoS attack mitigation service.
- Consider reducing your organisation's attack surface by:
  - outsourcing foundational online services (such as DNS) to reputable service providers who are able to withstand DoS attacks
  - partitioning critical online services (such as email) from other online services that are more likely to be targeted (such as websites)
  - ensuring that the DoS attack mitigation service only permits network traffic associated with the online service's network port(s).
- Discuss with your service providers the details of their DoS attack prevention and mitigation strategies, specifically their:
  - proven capability to withstand DoS attacks from around the world
  - demonstrated history of handling both DoS attacks and comprehensive authorised DoS attack testing
  - ability to automatically mitigate most types of DoS attacks without human involvement, such as manual analysis of network traffic
  - approach to pricing their services, such as whether the cost is fixed or it varies based on the amount of network traffic and computer processing resources used, and whether you can set a billing limit
  - thresholds for notifying you or turning off their online services during DoS attacks
  - pre-approved actions that can be undertaken during DoS attacks
  - DoS attack prevention arrangements with upstream providers.
- Implement measures to detect DoS attacks, such as real-time monitoring and alerting of system availability, network traffic, computer processing resources, and associated costs.
- Prepare a static version of your website that requires minimal processing and bandwidth to facilitate continuity of service during DoS attacks.
- Procure and use highly resilient online services with large bandwidth, adequate computer processing resources, geographically dispersed hosting locations and cloud-based traffic scrubbing to discard undesirable network traffic – this commonly includes using a reputable CDN to cache static website content and protect your origin web server from unwanted network traffic.
- Protect your organisation's domain names by using registrar locking, confirming domain registration contact details and other details are correct, and following additional guidance outlined in ASD's *Domain Name System security for domain owners* publication.
- Maintain up-to-date contact details for your service providers and share your organisation's contact details with them, ensuring all contacts are available based on your organisation's requirements, for example, 24 hours a day, 7 days a week.
- Provide your organisation's out-of-band contact details for a trustworthy communication channel to your service providers, for when normal communication channels fail.
- Develop, implement and maintain a cybersecurity incident response plan, covering various types of DoS attacks against each of your online services required to withstand DoS attacks, and exercise the plan at least annually.
- Architect applications to protect commonly abused functionality that consumes increased computer processing resources or that incurs additional financial costs (such as sending SMS messages).
  - Protections include rate limiting and verifying that requests are from a human.
  - Perform DoS attack testing including targeting improper logic flows in application functionality.
  - Perform broader load testing to identify and remediate DoS vectors.

Responding to DoS attacks

If your organisation has not prepared for DoS attacks, you can attempt to implement some of the above measures during DoS attacks, though they might be less effective and take time to implement, reducing your organisation's ability to respond.

Your organisation should implement the following measures during DoS attacks, where appropriate and practical.

- Enact your cybersecurity incident response plan.
- Ask your service providers if they are able to immediately implement responsive actions – if you have not previously discussed their ability to respond, you might discover that they are unable or unwilling to respond, or charge additional fees.
- Disable non-vital functionality or remove non-vital content from your online services that make the current DoS attack effective, for example, deploy a version of your website without search functionality, dynamic content or large files.
- Maintain communication with your customers and your service providers, including your DoS attack mitigation service provider, and continue monitoring the availability of your online services.
- Consider changing the IP address of your origin web server if it is being directly targeted, and avoid public disclosure of the new IP address without having protections in place.
- Report the DoS attack to relevant parties, including ASD and NCSC-NZ as per the 'Contact details' section of this publication.

Avoiding contributing to DoS attacks

Your organisation should implement the following measures to avoid unintentionally contributing to DoS attacks that could impact others.

- Avoid exposing services, IoT devices and other internet-connected devices to the internet which are unneeded, insecurely configured or inadequately maintained.
- Securely configure, maintain and monitor services, IoT devices and other internet-connected devices that are exposed to the internet.
  - Additional guidance for small businesses is available in ASD's *Internet of Things devices* and *Secure your Wi-Fi and router* publications.

If your organisation is running online services, you should implement the following additional measures.

- Prioritise reviewing protocols outlined in the United States' Cybersecurity and Infrastructure Security Agency's (CISA) *UDP-Based Amplification Attacks* advice.
- Monitor for new amplification vectors as they are identified and secure your online services against them.
- Configure both inbound and outbound network access controls to limit access to authorised online services and organisations.
- Block anonymous public access for amplification-prone online services if not required.
- Consider implementing a rate-limiting mechanism to reduce the consequences of abuse, if blocking or applying access controls is not possible or appropriate.

Further information

ASD's *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with the Essential Eight, complements this framework.

The *New Zealand Information Security Manual* is the New Zealand Government's manual on information assurance and information systems security. It is a practitioner's manual designed to meet the needs of agency information security executives as well as vendors, contractors and consultants who provide services to agencies.

More information on various DoS attack types is available in CISA's *DDoS Quick Guide* and *Understanding and Responding to Distributed Denial-Of-Service Attacks* publications.

Contact details

In Australia, if you have any questions about this guidance write to ASD or call 1300 CYBER1 (1300 292 371).

In New Zealand, to report a cybersecurity incident email incidents@ncsc.govt.nz or visit NCSC-NZ's Report an incident webpage.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre