Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Preparing for and Responding to Denial-of-Service Attacks

JUNE 2020

Introduction

Denial-of-service attacks are designed to disrupt or degrade online services such as website, email and DNS services. To achieve this goal, adversaries may use a number of approaches to deny access to legitimate users of online services such as:

- using multiple computers to direct a large volume of unwanted network traffic at online services in an attempt to consume all available network bandwidth
- using multiple computers to direct tailored traffic at online services in an attempt to consume the processing resources of online services
- hijacking online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

Although organisations cannot avoid being targeted by denial-of-service attacks, there are a number of measures that organisations can implement to prepare for and potentially reduce the impact if targeted. Preparing for denial-of-service attacks before they occur is by far the best strategy, it is very difficult to respond once they begin and efforts at this stage are unlikely to be effective.

While an organisation's primary focus is likely to be preventing themselves from being a victim of denial-of-service attacks, all organisations can take steps to ensure that their own online services cannot be abused by an adversary to conduct denial-of-service attacks targeting others.

Preparing for denial-of-service attacks

Before implementing any measures to prepare for denial-of-service attacks, organisations should determine whether a business requirement exists for their online services to withstand denial-of-service attacks, or whether temporary denial of access to online services is acceptable to the organisation.

If organisations wish to increase their ability to withstand denial-of-service attacks, they should, where appropriate and practical, implement the following measures prior to any denial-of-service attacks beginning:

- Determine what functionality and quality of service is acceptable to legitimate users of online services, how to maintain such functionality, and what functionality can be lived without during denial-of-service attacks.
- Discuss with service providers the details of their denial-of-service attack prevention and mitigation strategies. Specifically, the service provider's:
    - capacity to withstand denial-of-service attacks
    - any costs likely to be incurred by customers resulting from denial-of-service attacks

  - thresholds for notifying customers or turning off their online services during denial-of-service attacks
  - pre-approved actions that can be undertaken during denial-of-service attacks
  - denial-of-service attack prevention arrangements with upstream providers (e.g. Tier 2 service providers) to block malicious traffic as far upstream as possible.
- Protect organisation domain names by using registrar locking and confirming domain registration details (e.g. contact details) are correct.
- Ensure 24x7 contact details are maintained for service providers and that service providers maintain 24x7 contact details for their customers.
- Establish additional out-of-band contact details (e.g. mobile phone number and non-organisational email) for service providers to use when normal communication channels fail.
- Implement availability monitoring with real-time alerting to detect denial-of-service attacks and measure their impact.
- Partition critical online services (e.g. email services) from other online services that are more likely to be targeted (e.g. web hosting services).
- Pre-prepare a static version of a website that requires minimal processing and bandwidth in order to facilitate continuity of service when under denial-of-service attacks.
- Use cloud-based hosting from a major cloud service provider (preferably from multiple major cloud service providers to obtain redundancy) with high bandwidth and content delivery networks that cache non-dynamic websites. If using a content delivery network, avoid disclosing the IP address of the web server under the organisation's control (referred to as the origin web server), and use a firewall to ensure that only the content delivery network can access this web server.
- Use a denial-of-service attack mitigation service.

Responding to denial-of-service attacks

Organisations that wish to attempt to withstand denial-of-service attacks, but have not pre- prepared should, where appropriate and practical, implement the following measures, noting that they will be much less effective than had they been able to adequately prepare beforehand:

- Discuss with service providers their ability to immediately implement any responsive actions, noting service providers may be unable or unwilling to do so, or may charge additional fees for services not covered in contracts.
- Temporarily transfer online services to cloud-based hosting hosted by a major cloud service provider (preferably from multiple major cloud service providers to obtain redundancy) with high bandwidth and content delivery networks that cache non-dynamic websites. If using a content delivery network, avoid disclosing the IP address of the origin web server, and use a firewall to ensure that only the content delivery network can access this web server.
- Use a denial-of-service attack mitigation service for the duration of the denial-of-service attacks[1] [2].
- Deliberately disable functionality or remove content from online services that enable the current denial-of-service attack to be effective (e.g. implement a pre-prepared low resource version of the website, remove search functionality, or remove dynamic content or very large files).

[1] https://www.reuters.com/article/us-cyber-ddos/ddos-cyber-attacks-get-bigger-smarter-more-damaging-idUSBREA240XZ20140305
[2] https://www.wired.com/story/github-ddos-memcached/

Avoiding contributing to denial-of-service attacks

Organisations should ensure that they are not unwittingly contributing to denial-of-service attacks which could impact other organisations and/or individuals. In doing so, a key risk is the exposure of improperly configured or protected services which can be abused as part of a traffic amplification attack.

To ensure that the risk to others is minimised, organisations should implement the following measures:

- prioritise the review of protocols as outlined in the US-CERT ***UDP-Based Amplification Attacks*** publication at https://www.us-cert.gov/ncas/alerts/TA14-017A
- monitor for new amplification vectors as they are identified and review accordingly
- configure both inbound and outbound network access controls to limit access to authorised services and entities
- if not required, block anonymous public access of amplification-prone services
- if blocking or applying access controls is not possible or appropriate, consider implementing a rate-limiting mechanism to reduce the consequences of abuse
- if possible, secure the configuration of exposed services at the application level to limit the risk of abuse.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

For an overview of various denial-of-service attack types, broken down by network and application layer, refer to the US-CERT ***DDoS Quick Guide***. This publication can be found at https://www.us-cert.gov/security-publications/DDoS-Quick-Guide.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.