OCTOBER 2014

# Preparing for and Responding to Denial of Service Activities

## Introduction

1. Denial of service activities are designed to disrupt or degrade an organisation's online services such as their website, email and DNS services. To achieve this goal, adversaries may use a number of approaches to deny access to legitimate users such as:

   a. using multiple computers to launch a large volume of unwanted network traffic at an organisation's online services in an attempt to consume all available network bandwidth

   b. using multiple computers to launch tailored traffic at an organisation's online services in an attempt to consume the processing resources of online services

   c. hijacking an organisation's online services in an attempt to redirect legitimate users away from those services to other services that the adversary controls.

**Example**

During the 2012 G20 Leaders Summit in Mexico, the official website was unavailable for part of the Summit due to denial of service activities. The activist group Anonymous claimed responsibility for this disruption.

2. Although denial of service activities cannot be prevented from occurring, there are a number of measures that an organisation can implement to prepare for and potentially reduce their impact if they occur. Preparing for denial of service activities before they occur is by far the best strategy. It is very difficult to attempt to respond once they begin and efforts at this stage are unlikely to be effective.

## Preparing for Denial of Service Activities

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

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

a. 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 activities.

b. Discuss with service providers the details of their existing denial of service strategies. Specifically, the service provider's:

   i. capacity to withstand denial of service activities

   ii. any costs likely to be incurred by customers resulting from denial of service activities

   iii. thresholds for notifying customers or turning off their online services during denial of service activities

   iv. pre-approved actions that can be undertaken during denial of service activities.

c. Protect organisation domain names by using registrar locking and confirming domain registration details (e.g. contact details) are correct.

d. Ensure 24x7 contact details are maintained for service providers and that service providers maintain 24x7 contact details for their customers.

e. 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.

f. Implement availability monitoring with real-time alerting to detect attempted denial of service activities and measure their impact.

g. Partition critical online services (e.g. email services) from other online services that are more likely to be targeted (e.g. web hosting services).

h. 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.

i. Use a denial of service mitigation service [1].

## Responding to Denial of Service Activities

5. Organisations that wish to attempt to withstand denial of service activities, 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:

[1] http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305

a. 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.

b. Temporarily transfer online services to 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 origin web server, and use a firewall to ensure that only the content delivery network can access this web server.

c. Use a denial of service mitigation service for the duration of the denial of service activities[2].

d. Deliberately disable functionality or remove content from online services that enable the current denial of service activity to be effective e.g. removing search functionality, dynamic content or very large files from a website.

## Further Information

6. The *Australian Government Information Security Manual* (ISM) assists in the protection of government information that is processed, stored or communicated by Australian Government systems. The ISM can be obtained from http://www.asd.gov.au/infosec/ism/.

## Contact Details

7. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

8. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.

[2] http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305