NCSC Security Advisory **06 May 2015**

Denial of Service Extortion Campaign Targeting New Zealand Organisations

The NCSC is aware of an extortion campaign currently targeting New Zealand organisations. Several organisations have received extortion emails threatening a sustained Denial of Service attack (DoS)[1] unless a payment is made to the email sender. To demonstrate that the threat is credible, shortly after receiving the extortion email, the organisations are then hit with a short-duration DoS attack, lasting up to an hour. This short-duration DoS attack prevents access to the victim organisations' website.

Whilst investigations into this campaign continue, the NCSC is not currently aware of any instances where the threat to carry out a more sustained attack has been realised.

Preparation is the most effective method of withstanding a DoS attack. However, if your organisation is currently being targeted, there are a number of measures you can consider taking to reduce the impact of the attack.

- Contact your Internet Service Provider to discuss their ability to help you manage or mitigate the attack.
- Where applicable, temporarily transfer online services to cloud-based hosting providers that have the ability to withstand DoS attacks.
- Use a denial of service mitigation service for the duration of the DoS attack.
- Disable website functionality or remove content that is being specifically targeted by the DoS attack. For example, search functionality, dynamic content or large files.

If your organisation receives this type of attack, or if you have any further queries, please feel free to contact the NCSC on incidents@ncsc.govt.nz.

[1] A Denial of Service (DOS) attack is designed to disrupt or degrade an organisation's online services, such as their website.

P O Box 12-209, Wellington, New Zealand | incidents@ncsc.govt.nz | Phone: +64 4 498 7654 | Fax: +64 4 498 7655