National Cyber Security Centre

Cyber Security Advisory

CSA-007-16

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

03 May 2016

Distributed 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 Distributed Denial of Service attack (DDoS) unless a payment in Bitcoins is made to the email sender.

The NCSC is not currently aware of any instances where the threat to carry out an attack has been realised.

Any organisation receiving an extortion email should report the threat to their local police http://www.police.govt.nz/contact-us/stations.

We also recommend speaking with your Internet Service Provider (ISP) regarding advice and any specific DDoS mitigations that may be needed.

Preparation is the most effective method of withstanding a DDoS 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 DDoS attacks.
- Use a denial of service mitigation service for the duration of the DDoS attack.
- Disable website functionality or remove content that is being specifically targeted.

The NCSC can be contacted by email via ***incidents@ncsc.govt.nz*** *or by phone on:* ***04 498 7654****. We encourage you to contact us at any time if you require any further assistance or advice.*