National Cyber Security Centre

General Security Advisory

GSA-2018-582

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

17 August 2018

The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Ongoing use of Business Email Compromises to facilitate fraud

Summary

The NCSC is aware of New Zealand organisations business email accounts being compromised and used to facilitate fraudulent payments. Criminals undertaking this activity gain access to an organisation's email account to change or create illegitimate business-to-business transactions for their own financial gain. The account can be compromised for some time before criminals choose to act, using one or more of the following techniques:

- The criminal intercepts a legitimate email chain between two organisations discussing payment for goods or services. The criminal then replies, using the organisation's compromised email account, with the criminal's own bank account details. To the recipient, it appears as part of the existing email chain.
- The criminal edits an organisation's legitimate invoice, inserting the criminal's own bank account details. The criminal then uses the organisation's compromised email account to send the fraudulent invoice to customers or suppliers.

The financial impact of these techniques can be severe but organisations can manage this risk using a range of technical and internal financial controls.

Recommendations

The initial compromise and access to an organisation's emails can occur in a number of ways. For example, phishing emails with links to credential harvesting pages and persistent brute force attempts against known accounts are two common techniques.

The NCSC recommends organisations take steps to protect their business email accounts against this compromise:

- Enable Multi-Factor Authentication. This could include:
    - A mobile app (online and one-time password) as a second authentication factor.
    - A phone call as a second authentication factor.
    - A text message as a second authentication factor.
- Review email logging information for any unusual logins.
- Review email forwarding rules for any unknown configurations within accounts.
- Inform end users about the increased likelihood of phishing emails and undertake security best practices when receiving unknown emails.

Organisations should ensure they have internal financial controls appropriate to the size and nature of their business to prevent and detect fraudulent payment requests. Organisations should work with their financial advisors and auditors to review and test these internal financial controls. Internal controls that would have mitigated recent instances of payment fraud include:

- Confirming bank account details received in an email concerning large financial transactions via another source (by phone, for example).
- Considering the requirement to have transactions over a certain value reviewed and authorised by at least two individuals within an organisation.

These common business practices would help to mitigate the risk of falling victim to a fraudulent payment request based on a business email compromise.

*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.*