17 August 2015

NCSC Security Advisory - NCSC-EV-2015-126

Spear Phishing Emails Used for Credential Harvesting Across Mulitple Government Agencies

WARNING: *This alert is for computer network defence purposes only. Further dissemination and information extraction, including to other New Zealand government agencies or vendors requires the permission of the originator.*

The NCSC is aware of a recent campaign involving credential harvesting attacks in the form of spear phishing emails targeting a number of different government agencies.

The attack is delivered using a spear phishing email containing a malicious link, different social engineering techniques to fool the victim and/or compromising legitimate email accounts to propagate further. If a user visits the link they will typically be sent on a redirect chain until they end on a webpage (Figure 1).

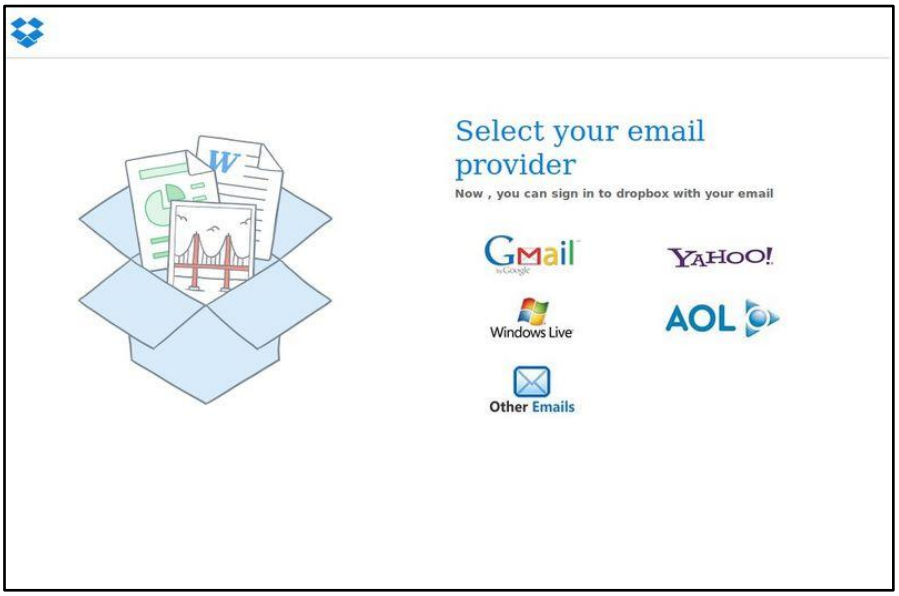

Figure 1 - Credential Harvesting Landing Page

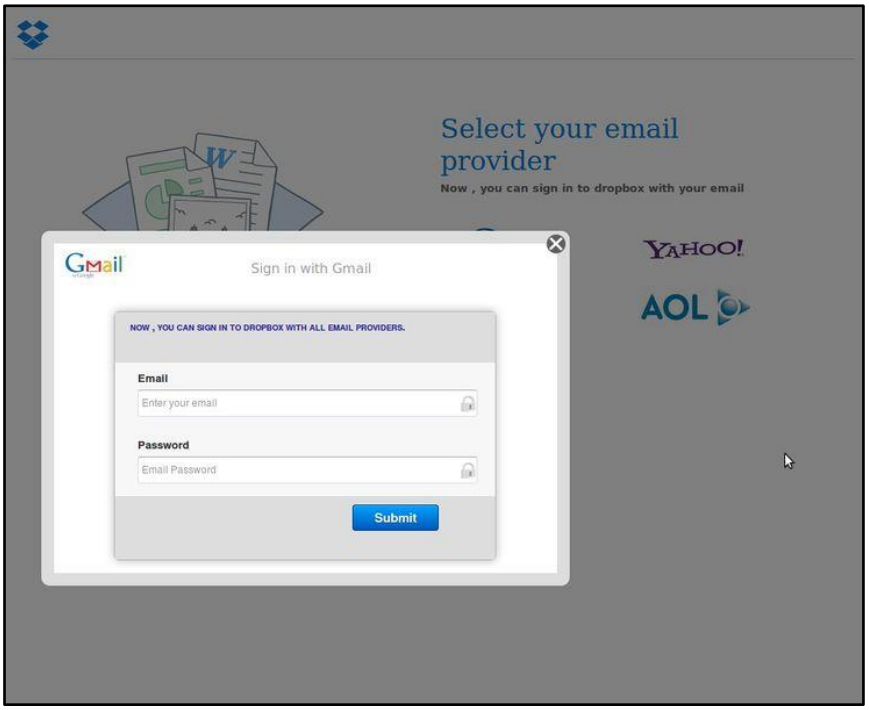

Figure 2 - Credential Harvesting Email Selected

The user's credentials can be stolen in one of two ways. The first method requires the user to enter their details into the email and password fields and click "Submit" (Figure 2). The second method will hijack the user's browser cookies which contain usernames, passwords and session ID's.

Once an email account has been compromised, the attacker has full access to the account and is able to resend malicious links to any email address in the address book. These emails will usually only contain a single link with no text but can trick a victim into visiting as it has come from one of their legitimate contacts.

For previously reported credential harvesting attacks please refer to NCSC Security Advisory NCSC-C-2014-17 (12th August 2014).

The NCSC strongly recommends advising all employees not to reply to the email, not to follow the link and/or enter any details in the corresponding webpage. Remind employees to check if the webpages they visit correspond to the URL. If an employee has previously entered their details or has received an email that fits the advisory's description then they are advised to contact their IT Security Team immediately.

In addition, any password reset should be done from the mail client, rather than clicking on a link in an email. To help stop propagation, check mail settings to ensure auto forwarding is disabled.

The NCSC can be contacted by email via incidents@NCSC.govt.nz or by phone on: 04 498 7654.

Any emails matching this description that have been received but not opened should be logged and deleted immediately. It is important that there is no attempted interaction with the email originator.

The NCSC urges all New Zealand government agencies and employees to be extremely cautious when in receipt of emails from unfamiliar addresses or email providers, even if they appear legitimate at first glance. If unsure of an attachment, contact the sender of the email by other trusted means to verify that this was in fact sent by the person.

Spear phishing poses a significant threat to New Zealand's cyber security and the NCSC encourages measures to ensure government employees are aware of the risks posed by unsolicited emails directed at them from external sources.

Do not attempt to conduct queries, probes or scans on the entities, techniques, domains, URL's IP addresses or other intrusion identifiers contained in this advisory. Such actions may alert hostile entities, harm information systems and/or produce false positives.