UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00076

ZOOM IMPERSONATION PHISHING CAMPAIGN

DATE ISSUED: 7th December 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A new phishing campaign has been spotted by the Better Business Bureau impersonating Zoom, complete with the company logo, through email, text and social media messages as the Covid-19 pandemic continues to necessitate working remotely.

BREAKDOWN

Users are receiving impersonation emails containing a malicious link stating that their Zoom account is soon to be suspended or that they have missed a meeting. This link, when clicked, redirects the user to a landing page where they are prompted to enter their credentials to log in to reschedule their meeting or restore their access. The most recent slew of emails that have been seen are fake welcome emails asking users to activate their accounts by accessing the malicious link. A total of 2,449 malicious Zoom impersonation domains have been registered since April 2020. These links may be used for credential harvesting in an effort to discover if the password has been re-used across other accounts and gain access to those, or install malware on the users device, or both, and can be used to perform "Zoom-bombing" attacks to gain unauthorised access to meetings.

REMEDIATION STEPS

- Be wary of any emails containing links and refrain from clicking them
- Educate users to recognise key signs of phishing attacks
- Do not re-use passwords across various accounts
- Ensure all passwords are long, complex, and align with company policies and standards
- Restrict access to Zoom meeting by utilising the waiting room feature for all meetings to admit access

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/zoom-impersonation-attacks-credentials/161718/