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

CYBER GUIDANCE ISSUE 00222

PROOFPOINT BRAND USED BY PHISHING SCAMMERS

DATE ISSUED: 10th November 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A recent phishing campaign has been spotted that impersonates the well-known cybersecurity company Proofpoint in an effort to harvest Microsoft o365 and Google account credentials, allowing attackers to bypass email security checks.

BREAKDOWN

An email has is sent claiming to contain a secure file from Proofpoint accessible through the hyperlink embedded in the email message. The campaign contained Proofpoint branding and logon links for the relevant email provider in the targeted organisation, making the email seem more legitimate to users. Users who accessed the link were directed to a specially crafted login page for Microsoft or Google, where a user could "login" and in this case, have their credentials harvested. The subject line appears as a reply using the Re: prefix, attempting to dupe recipients into thinking the message was part of an on-going conversation. This sophisticated attack replicated workflows commonly present for users to increase the appearance of authenticity. Attackers had compromised a legitimate email to disperse their campaign from, which meant email security filters allowed the malicious emails through. Phishing pages were hosted on a .co.uk domain registered in April 2021 called greenleafproperties which redirects to cvgproperties – a barebones website which suggests it may be a dummy site.

REMEDIATION STEPS

- Educate users about social engineering, brand impersonation, and phishing emails and instruct them on what to do if they believe they have received a suspicious email within your organisation.
- Ensure good password practices and policies are in place within your organisation.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/proofpoint-phish-microsoft-o365-google-logins/176038/
IT Pro https://www.itpro.co.uk/security/cyber-security/361477/proofpoint-impersonator-grabs-microsoft-365-and-google-logins-in
Security Boulevard https://securityboulevard.com/2021/11/proofpoint-phishing-attack-shows-why-every-ciso-needs-to-protect-against-brand-impersonation/