UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00123

O365 PHISHING TARGETS FINANCIAL EXECS

DATE ISSUED: 22nd March 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Phishing is set to be one of the top threats of 2021 and attackers are moving away from targeting CEO's to set their sights on Financial Executives instead, such as the Chief Financial Officer (CFO) and other execs using Microsoft Office 365 themed campaigns.

BREAKDOWN

Not only are executives facing this type of threat, but their assistants are also set to be in the firing line based on observations of a slew of recent phishing campaigns set to harvest Microsoft Office 365 credentials and other sensitive information. Seeking to achieve Business Email Compromise (BEC), attackers are targeting financial departments in an effort to gain access to invoicing, account and third-party information and use the compromised account, send legitimate seeming emails to suppliers and customers requesting payments to achieve financial gains. The attacks seen thus far are using Microsoft branding and seemingly legitimate content, such as requiring an update from the user, sent from imposter Microsoft domains or by spoofing email addresses of known senders to avoid detection by email security technologies and the user. These fraudulent domains tend to disappear as quickly as they emerge to avoid traceability. Once accessed, victims are redirected to malicious sites and asked to accept a 'Privacy Statement' after which they are redirected further and prompted to log in. In some cases, the attacks have been far more sophisticated, incorporating localised Office sign-in, even circumventing SSO and ADFS in some cases.

REMEDIATION STEPS

- Educate users on the dangers of phishing emails – particularly those containing hyperlinks, require downloads or that request a user to sign-in to an application or service via hyperlink. Teach them how to spot phishing emails and what to do with emails they believe are suspicious in your organisation.
- Use SPAM filtering and Secure Email Gateways to reduce the likelihood of phishing emails reaching users.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/office-365-phishing-attack-financial-execs/164925/

Trend Micro https://www.trendmicro.com/en_us/research/21/a/fake-office-365-used-for-phishing-attacks-on-c-suite-targets.html