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

CYBER GUIDANCE ISSUE 00046

ATTACKERS USE CAPTCHA FOR PHISHING

DATE ISSUED: 5th October 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

In a recent phishing campaign aimed at stealing Microsoft Office 365 credentials, attackers used a triple CAPTCHA to make the request for credentials seem legitimate and snare more victims.

BREAKDOWN

CAPTCHA's are used on websites in order to make sure it is a human interacting with them, rather than a robot or website crawler and are often implemented as a method of assuring users that the website they are using is secure. In a recent phishing campaign aimed at stealing Microsoft 365 credentials, researchers saw a three-step CAPTCHA on the landing page when a user accessed the malicious site, where the user was prompted to use the confirmation tick box and two image identification screens. Thereafter they were asked to enter their Microsoft 365 credentials which were then acquired by the attackers. Using common security controls against users is not ground-breaking news, however the efficiency of this campaign has highlighted the dangers in trusting known security tools like CAPTCHA implicitly. With phishing continuing to be the most used and most successful attack methods used today and with volume of attacks set to rise, as well as greater sophistication of attacks, social engineering is continuing to be quite a headache for cyber security professionals.

REMEDIATION STEPS

- Conduct user awareness training in a variety of forms within your organization
- Educate users about how to identify suspicious emails and URLs
- Provide a means for users to report suspicious emails for investigation
- Ensure URL filtering is enabled on your network to prevent access to known malicious sites.
- Using Secure Email Gateway Software and SPAM filtering to reduce the volume of suspicious emails that will reach the end user and reduce potential risk.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/microsoft-office-365-captchas/159747/
Helpnet Security: https://www.helpnetsecurity.com/2020/05/01/recaptcha-walls/
Cofense https://cofense.com/new-phishing-campaign-uses-captcha-bypass-email-gateway/