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

CYBER GUIDANCE ISSUE 00056

MICROSOFT TEAMS UNDER PHISHING THREAT

DATE ISSUED: 27th October 2020

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

OVERVIEW

"Missed chat" notifications are being used to dupe Microsoft Teams users into revealing their login credentials in a current phishing campaign.

BREAKDOWN

Using this popular collaboration tool as its guise, an email is sent to users notifying them of either new activity in teams or a missed chat message. Due to the rise in popularity of this software as a remote working tool, coupled with the way user quickly interact with chatting applications, attackers assumed it would be an apt method to lower normal user security checks regarding phishing emails. Three links were seen to be present in the emails and all three lead to credential harvesting phishing pages. A great deal of care was taken in the creation of both the phishing emails and the login pages to appear legitimate in the "spray" tactic campaign. Microsoft applications and 365 credentials continue to be the most targeted brand for phishing impersonation.

REMEDIATION STEPS

- If in doubt, access the application through alternative channels, such as through the application or by typing in the correct URL.
- Be wary of minor errors in any URL accessed through an email – such as missing a "." In the appropriate place or the use "vv" instead of "w" for example
- Check for the HTTPS padlock icon in the address bar of the browser when accessing websites.
- Use URL filtering for known malicious sites.
- Turn off "Missed Activity" email notifications for Microsoft Teams

REFERENCES & RESOURCES

Threatpost https://threatpost.com/microsoft-teams-phishing-office-365/160458/
SC Magazine https://www.scmagazine.com/home/security-news/vulnerabilities/attackers-prey-on-microsoft-teams-accounts-to-steal-credentials/
Abnormal Security https://abnormalsecurity.com/blog/microsoft-teams-impersonation/