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

CYBER GUIDANCE ISSUE 00091

MFA BYPASSED IN CLOUD-BASED ATTACKS

DATE ISSUED: 18th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Opportunistic malicious actors are discovering and exploiting numerous ways to bypass Multi-Factor Authentication (MFA), also known as Two-Factor Authentication (2FA) for cloud services with poor cyber hygiene and misconfigurations.

BREAKDOWN

So far, these attacks have been observed when users are using a hybrid of organisation issued and personal devices to work remotely and gain access to their cloud services. An example of poor cyber hygiene included the lack of use of a VPN to access these services and an open port 80 on the server to support working from home practices. Email phishing for credential harvesting and "pass the cookie" session hijacking attacks have also been noted as potential vectors by social engineering and exploiting browser storage of authentication information. Further email exploitation included the abuse of forwarding rules once an account has been compromised to redirect mail to an attacker's account to prevent warnings from alerting the user of potential compromise. Attackers are suspected to be using numerous methods to hide their own location.

REMEDIATION STEPS

- Re-evaluate secure remote access practices and ensure all staff are using technologies such as VPN to remotely log in to any cloud service or other devices located on the corporate network.
- Ensure staff are using corporate devices rather than personal devices for access to corporate networks and services.
- Educate users around the dangers and consequences of phishing and social engineering and put processes in place for reporting suspected incidents.
- Check security configurations on all cloud services including user permissions.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/cloud-attacks-bypass-mfa-feds/163056/