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

CYBER GUIDANCE ISSUE 0320

COMPROMISED M365 ACCOUNTS PHISHING CAMPAIGN

DATE ISSUED: 1st June 2023

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

OVERVIEW

Compromised Microsoft 365 accounts are being leveraged in a targeted phishing attack to steal sensitive system information and Microsoft credentials. A phishing email containing encrypted Restricted Permission Message Files (RPMSG) is able to evade email scanning gateways as the embedded .rpmsg messages and including URL links are encrypted.

BREAKDOWN

Researchers at Trustwave recently discovered new phishing attacks involving a combination of compromised Microsoft 365 accounts and '.rpmsg' (Restricted Permission Message Files) encrypted emails to deliver a phishing message. The attack starts with an email containing a Microsoft encrypted message originating from a compromised Microsoft 365 account. Users are prompted to click a "Read the message" button to view the encrypted message, redirecting them to a legitimate Office 365 login page. After authenticating, users can see the phishing email that redirects them to a fake SharePoint document hosted on Adobe's InDesign service where they click a "Click here to Continue" button. From there, clicking "Click Here to View Document" leads to the destination that displays an empty page and a "Loading...Wait" message that acts as a decoy to allow a malicious script to harvest sensitive system information. It may include visitor ID, connect token and hash, video card renderer information, system language, device memory, hardware concurrency, installed browser plugins, browser window details, and OS architecture. Once the script collects the targets' data, the page will show a cloned Microsoft 365 login form to send the entered usernames and passwords to the Command-and-Control Servers (C2C).

REMEDIATION STEPS

- Security awareness training is essential for training employees to recognise and avoiding phishing threats.
- Educate users on the nature of the threat, and not to attempt to decrypt or unlock unexpected messages from outside sources.
- Enable multi-factor authentication (MFA) on all applications and services.
- Adopt a defence-in-depth strategy by implementing Next Generation endpoint security solutions such as email and web filtering to block the initial phishing email.

REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/microsoft-365-phishing-attacks-use-encrypted-rpmsg-messages/

Trustwave https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/microsoft-encrypted-restricted-permission-messages-deliver-phishing/