UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00205

FLUBOT REACHES NZ & TARGETS ANDROID PHONES

DATE ISSUED: 4th October 2021

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

OVERVIEW

As mentioned in the TangleBot Cyber Guidance update (Cyber Guidance Issue 0204), FluBot malware has hit New Zealander's this week and is being spread via SMS messages to Android mobile phones. These messages come in three forms – a parcel pending delivery, an attempted photo album share or a received voicemail.

BREAKDOWN

Users who receive the SMS messages does not mean that the malware has been installed on user's devices. The link contained within the text message redirects the user to a page that states their device has been infected by FluBot malware – this is not the case. The webpage then prompts the user to follow instructions to remove the malware and download a security update. It is at this stage if a user follows the instructions, accesses any further links or downloads any packages that the malware will be installed on the device. FluBot is a botnet malware that will attempt to exfiltrate user data and upload it to the C2 (Command and Control) Server and will use the contacts stored in the phone and its apps to continue to propagate the malware. The messaging in the malicious texts started as the parcel pending notification and the two other variants quickly appeared, so it is likely that new messages will continue to appear to avoid suspicious and heighten the likelihood of a user taking the bait. FluBot also blocks the number once the text message is sent so a user is unable to reply to the original message.

REMEDIATION STEPS

- Do not click links in SMS messages. This should also apply to messages receive over social media or messaging applications – particularly if they are unexpected
- If you are expecting a delivery, it is best to track it via the couriers website by typing the URL into the address bar of your browser.
- Forward any suspicious texts to CERT NZ through 7726.
- If you believe your device has been infected:
    - Perform a factory reset of the device to delete all personal data.
    - Do no restore from backups that were created after the app had been installed, it is recommended you use a prior version of your backups.
    - Change passwords to all of your online accounts – particularly banking passwords and assess your account to verify there has been no unauthorised access. If you do suspect unauthorised access, contact your bank immediately.

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/individuals/alerts/flubot-malware-infecting-android-phones/
Threatpost	https://threatpost.com/flubot-malware-targets-androids-with-fake-security-updates/175276/