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

CYBER GUIDANCE ISSUE 00040

ANDROID MALWARE EVOLUTION

DATE ISSUED: 28th September 2020

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

OVERVIEW

Following on from our Cyber Guidance Issue 0008 in July, the Cerberus banking Trojan has a new variant known as 'Alien' and has similar objectives to the parent malware, able to infiltrate over 200 applications and target the associated credentials and much more.

BREAKDOWN

With its ability to circumvent Multi-Factor Authentication (MFA), this newly evolved RAT attacks 226 different social media, banking, and email applications in search of login credentials. This Malware-as-a-Service (MaaS) has been seen to be used in actively targeting organizations worldwide, including incidents in Australia, and may be only a matter of time before it reaches us across the ditch. The "android.permission.BIND_NOTIFICATION_LISTENER_SERVICE" is leveraged to steal notifications and by elevating Accessibility privileges on the Android device, removes the requirement of user interaction and performs any necessary actions by itself. Using the advanced remote access features in TeamViewer, devices may be infiltrated and alter various settings without user knowledge or interaction to gain access to whatever it likes, such as banking applications. At this stage the distribution method of this malware is unclear, although it is suspected to be delivered through spear phishing emails and third party applications.

REMEDIATION STEPS

- Be wary when downloading any applications, particularly from unknown sources.
- Ensure mobile security anti-malware protections are in place on all Android devices connected to your organizations network.
- Perform regular monitoring and security checks on all Android devices to locate any suspicious activity
- Investigate and deploy a Mobile Device Management plan and solution

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/alien-android-2fa/159517/
Toms Guide: https://www.tomsguide.com/news/alien-android-malware
The Daily Mirror (UK) https://www.mirror.co.uk/tech/android-warning-alien-malware-discovered-22737323
ZDNet: https://www.zdnet.com/article/new-alien-malware-can-steal-passwords-from-226-android-apps/