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

CYBER GUIDANCE ISSUE 0008

ANDROID MALWARE ON GOOGLE PLAY

DATE ISSUED: 7th July 2020

OVERVIEW

The Google Play application marketplace has recently seen an increase in malware posing as legitimate applications,

BREAKDOWN

Malware is avoiding detections by posing as legitimate applications to avoid application filtering and checking processes, as well as developing fake GitHub profiles and backstories for developers like OceanLotus. Recently discovered Android malware includes the Cerberus banking Trojan that is able to bypass security measures such as multifactor authentication through the interception of text messages to enable the theft of credentials for bank account seizure. In its first stage posing as a legitimate, in the second stage becomes a "dropper" connecting to a command and control centre to download the Cerberus package. It has since evolved to include further information harvesting capabilities and the ability to run Team Viewer – a remote access tool. Haken exfiltration malware as well as PhantomLance and spyware campaigns have also recently been discovered in Google Play applications. The Joker (a.k.a Bread) malware has been continually adapted to circumvent detection since 2019, which exfiltrates sensitive information and subscribers users to premium subscriptions in an effort to cause financial loss to victims, rooting itself in the 'Android Manifest' device admin files.

REMEDIATION STEPS

- Research and vet new applications before installation and use sandbox environment for testing where possible
- Be aware of permission requests that may seem suspicious and deny access
- Use a mobile endpoint protection application and anti-malware software on any Android mobile devices
- Restrict BYOD devices from company networks and allow access to a separate purpose=built network only

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/cerberus-banking-trojan-unleashed-google-play/157218/
https://threatpost.com/sophisticated-android-spyware-google-play/155202/
https://threatpost.com/joker-android-malware-dupes-its-way-back-onto-google-play/157307/
Digital Trends https://www.digitaltrends.com/mobile/how-to-remove-malware-from-your-android-phone/