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

CYBER GUIDANCE ISSUE 00256

FACESTEALER TROJAN SPYS ON FACEBOOK ACCOUNTS

DATE ISSUED: 22nd March 2022

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

OVERVIEW

Craftsart Cartoon Photo Tools app available on the Google Play Store is the latest clever ruse for the Facestealer Android malware to steal login credentials and steal information from the unwitting downloader's Facebook account.

BREAKDOWN

Trojans are a type of malware that hides inside something seemingly legitimate – like a photo editing app in this example. The Craftsart Cartoon Photo Tools app has over 100,000 downloads on the Google Play Store and the small piece of malware contained within manages to slip past the store's security controls. Once launched, the app redirects the user to the real Facebook login page and requests the user login before they can use the app. The JavaScript code working in the background then steals the credentials and relays them to the C2 server which authorises access to the account. The malware then sets to work stealing the victim's personal information such as email addresses, IP addresses, phone numbers, conversation histories, friend lists and any credit card information it can find. As the attacker now has the login credentials for the account, they can use this for further reconnaissance and distribution of further attacks.

REMEDIATION STEPS

- Be wary of apps that ask for excessive permissions or access to another account (such as your Facebook account in this instance) before you can use the application or features.
- Always check user reviews and developer information – do your research

REFERENCES & RESOURCES

Threatpost https://threatpost.com/facestealer-trojan-google-play-facebook/179015/
Bleeping Computer https://www.bleepingcomputer.com/news/security/android-password-stealing-malware-infects-100-000-google-play-users/