TM-2020-017
MALICIOUS ANDROID APP THROUGH FRAUDULENT WEB CLAIMING FROM PERDANA MENTERI

Date: 3rd APRIL 2020

1.0 Introduction

On 2nd April 2020, National Cyber Coordination and Command Centre (NC4) has been informed of a malicious Android mobile app being distributed from fraudulent website claiming from Perdana Menteri Malaysia. The Android app serves a purpose for COVID-19 aid programme.

The malicious app enable victim to submit their banking details to attacker. Besides that, the malicious app is capable to read mobile phone SMS which can be use by attacker to steal the TAC codes for Internet banking.

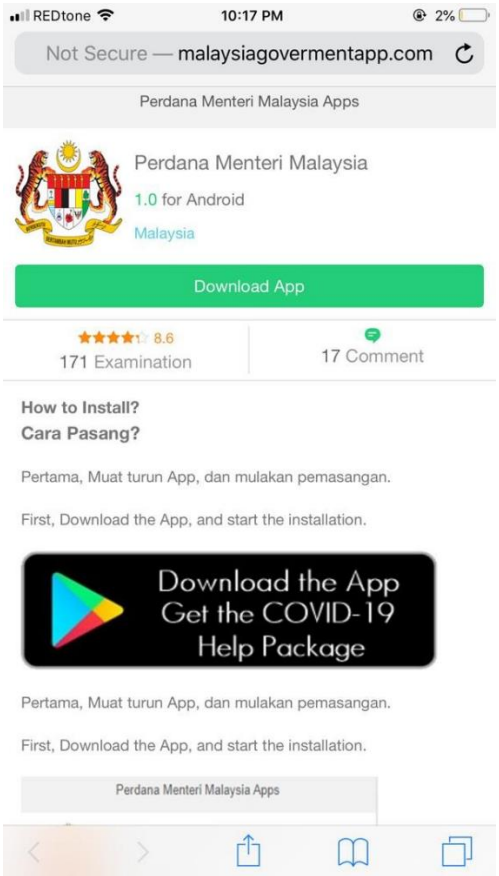

Image 1: Malicious App from fraudulent web link claiming from Malaysia government

2.0 Impact

1. Success exploitation resulting to identity theft and financial loss.

3.0 Recommendation

1. Do not install and click on any suspicious link.
2. Do not download any mobile apps from external link (e.g. from web, SMS and chat messaging) other than Google Play Store or the Manufacturer's App Stores such Apple AppStore, Huawei AppGallery, and Samsung Galaxy Store.
3. Official information regarding COVID-19 is send by MKN through mobile phone SMS will be tagged as "MKN" by the telco with no number to reply.
4. If you already installed the malicious app, removed the app; and informed your bank immediately to block the transaction and change the bank account access.
5. In the event of a host has been compromised, report immediately to socsirt@tm.com.my.

References

1. http://www.nc4.gov.my/view_alert_advisory?id=5e85fb35e4b0dfeff44f7497