



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


**Date: 3<sup>rd</sup> APRIL 2020**

**Confidentiality**

This document contains proprietary information that is confidential to Telekom Malaysia Berhad. Disclosure of this document, in full, or in part, may result in material damage to Telekom Malaysia Berhad. Written permission must be obtained from Telekom Malaysia prior to the disclosure of this document to any third party.

**Copyright and Disclaimer**

This document contains highly confidential and proprietary information of Telekom Malaysia Berhad. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the expressed written permission of Telekom Malaysia Berhad. Telekom Malaysia Berhad may have patents or pending applications, trademarks, copyrights, or other intellectual property rights covering subject matters in this document. The furnishing of this document does not give any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided for in any written license agreement with Telekom Malaysia Berhad.

	<b>GROUP INFORMATION SECURITY</b>	<b>Document No: TMA-2020-017</b>	Rev No :
			Date: 3/4/2020
<b>MALICIOUS ANDROID APP THROUGH FRAUDULENT WEB CLAIMING FROM PERDANA MENTERI</b>			Page 2 of 3

## 1.0 Introduction

On 2<sup>nd</sup> 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.

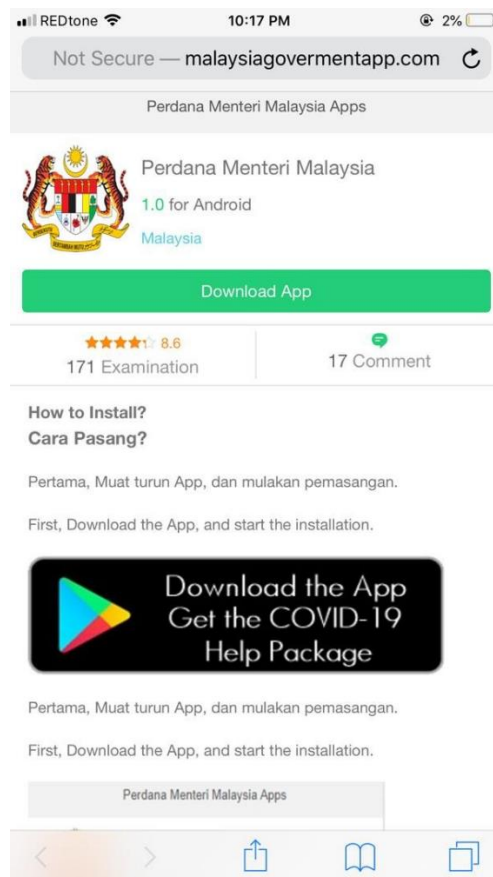



Image 1: Malicious App from fraudulent web link claiming from Malaysia government

## 2.0 Impact

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

	<b>GROUP INFORMATION SECURITY</b>	<b>Document No: TMA-2020-017</b>	Rev No :
			Date: 3/4/2020
<b>MALICIOUS ANDROID APP THROUGH FRAUDULENT WEB CLAIMING FROM PERDANA MENTERI</b>			<b>Page 3 of 3</b>

### 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 as 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](mailto:socsirt@tm.com.my).

### References

1. [http://www.nc4.gov.my/view\\_alert\\_advisory?id=5e85fb35e4b0dfeff44f7497](http://www.nc4.gov.my/view_alert_advisory?id=5e85fb35e4b0dfeff44f7497)