Telegram: **"CHIEFMIN KOTA KINABALU"**

BIL. JKM. 100-4/62

Tolong sebutkan rujukan fail kami dalam jawapan surat ini
(Please quote our file reference in your reply to this letter)

JABATAN KETUA MENTERI
(CHIEF MINISTER'S DEPARTMENT)
Aras 28, Blok A,
Pusat Pentadbiran Negeri Sabah
Jalan UMS, Teluk Likas
88400 KOTA KINABALU
Sabah, Malaysia

Tel.: 088-369900/369901
Faks: 088-211016

08 April 2020

Semua Setiausaha Tetap Kementerian;
Semua Ketua Jabatan Negeri;
Semua Pihak Badan Berkanun Negeri;
Semua Pihak Berkuasa Tempatan; dan
Semua Pegawai Daerah/Penolong Pegawai Daerah.

Yang Berbahagia Datuk/Tuan/Puan,

MAKLUMAN DAN PERINGATAN *(ALERT)* MENGENAI ANCAMAN SERANGAN SIBER KE ATAS AGENSI-AGENSI KERAJAAN SEMASA TEMPOH PERINTAH KAWALAN PERGERAKAN (PKP)

Perkara di atas dirujuk.

2. Untuk makluman, Agensi Keselamatan Siber Negara *(National Cyber Security Agency (NACSA))*, Majlis Keselamatan Negara (MKN) melalui *National Cyber Coordination and Command Centre (NC4)* telah mengesan beberapa serangan siber ke atas beberapa agensi Kerajaan. Sepanjang tempoh PKP, NC4 telah mengesan serangan siber oleh penggodam ke atas Kerajaan dan rakyat Malaysia. Jenis-jenis serangan yang dikesan merangkumi serangan *Advanced Persistent Threat (APT)* dan pencerobohan laman sesawang Kerajaan dan syarikat-syarikat swasta. Selain itu, terdapat insiden-insiden lain seperti penipuan atas talian, *email spam* dan aplikasi mudah alih palsu.

3. Peningkatan bilangan insiden pencerobohan terhadap pelayan agensi Kerajaan juga dikesan sepanjang tempoh PKP. Insiden pencerobohan ini melibatkan pencacatan laman sesawang dan sistem aplikasi di agensi. Sepanjang tempoh PKP ini, perkhidmatan sidang video digunakan secara meluas oleh semua rakyat yang bekerja di rumah. Salah satu aplikasi sidang video yang sering digunakan selain daripada Skype adalah aplikasi **Zoom**. Zoom ialah satu aplikasi sidang video web percuma. Aplikasi ini didapati mempunyai kelemahan yang membolehkan penggodam memanipulasi perisian tersebut untuk mencuri dengar perbualan pengguna.

..2/

4. Bersama-sama ini disertakan salinan notis amaran dan peringatan yang juga boleh dicapai melalui https://www.nacsa.gov.my/alert.php berkenaan dengan insiden-insiden yang dinyatakan di atas untuk tindakan dan rujukan pihak YBhg. Datuk/Tuan/Puan. Kerjasama daripada YBhg. Datuk/Tuan/Puan diminta untuk memaklumkan mengenai perkara ini kepada agensi-agensi di bawah seliaan.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

(DATUK HAJI SAFAR BIN UNTONG)
Setiausaha Kerajaan Negeri

s.k. Pengarah
Majlis Keselamatan Negara Negeri Sabah
Jabatan Perdana Menteri
Aras 6, Blok A, Kompleks Pentadbiran Kerajaan Persekutuan
Jalan UMS
88400 KOTA KINABALU

Advisory on Cyber Threat Using COVID19 Outbreak As Theme

Introduction:

The National Cyber Coordination and Command Centre (NC4) continuously monitor the cyber threat landscape that may affect national security both locally and globally. We have observed an increased number of cyberattacks, targeting multiple organisations worldwide, taking advantage of Coronavirus (COVID19) public health issue as a lure to attract victims to fall into their traps. With the recent announcement of Movement Control Order (MCO) by the Prime Minister of Malaysia, which requires all non-essential government and business premises to be closed from 18 to 31 March 2020, the NC4, National Cyber Security Agency (NACSA), National Security Council (NSC) would like to remind everyone to be vigilant and to continue to observe the cyber hygiene practices while working from home.

Impact:

Loss of information, service disruption, information exposure and financial loss.

Brief Description:

Following the COVID-19 outbreak, NACSA has observed several scams and malware activities that have employed the COVID-19 theme to lure victims to give out personal information and install malicious apps. Cyberattack campaigns, including Business Email Compromise, Malware, Ransomware and phone scams, are on the rise and are believed to be organized by APT groups and organised crime groups, leveraging on this situation for their latest campaigns.

Based on a report from Trend Micro, several malicious domains containing the word “corona” as part of the domain name have been identified and NC4 also has identified several malicious email subjects, attachments and malicious URLs that have used the word "COVID-19" and "coronavirus" in their phishing lures. The full list of malicious domains, email subjects and hashes are as in **Appendix 1** below. The content of the **Appendix 1** will be updated from time to time to reflect new indicator of compromise (IOC).

Recommendation:

The NC4 would like to advice organisations and individuals to take the following precautionary steps during this period of MCO:

1. to harden the ICT infrastructure that will support the Work-From-Home policy and the spike of online transactions from the public users;
2. to verify any information received from emails, text messages and social media posts regarding COVID-19;
3. to use Virtual Private Network (VPN) connections to access your internal resources;
4. to not open any suspicious links or emails;
5. to not visit any untrusted websites;
6. to not simply enter personal information, such as email address or password, whenever you are requested to do so;
7. to change your password if you think it is stolen;
8. to update your mobile phone and computer's operating system and applications regularly;
9. to apply the latest patches for your system and application to protect from being exploited;
10. to monitor your network traffic and block attempts to exploit your server and network;
11. be careful and verify any calls claiming from legal enforcement agencies, banks or companies that you may have been dealings with;
12. to contact law enforcement agency should you suspect that you have been a victim of a scam;
13. to block malicious emails with subjects and hashes listed in Appendix 1; and
14. to report to NACSA if your server has been breached or defaced.

Reference:

1. Coronavirus Used in Malicious Campaigns

   https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

2. Coronavirus Scams: Watch Out For These Efforts To Exploit The Pandemic

   https://www.forbes.com/sites/mattperez/2020/03/16/coronavirus-scams-watch-out-for-these-efforts-to-exploit-the-pandemic/#3047e9626103

3. Foreign APT groups use coronavirus phishing lures to drop RAT malware

   https://www.scmagazine.com/home/security-news/cybercrime/foreign-apt-groups-use-coronavirus-phishing-lures-to-drop-rat-malware/

4. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

   https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

Appendix 1

1) MALICIOUS DOMAINS:

- acccorona[.]com
- alphacoronavirusvaccine[.]com
- anticoronaproducts[.]com
- beatingcorona[.]com
- beatingcoronavirus[.]com
- bestcorona[.]com
- betacoronavirusvaccine[.]com
- buycoronavirusfacemasks[.]com
- byebyecoronavirus[.]com
- cdc-coronavirus[.]com
- combatcorona[.]com
- contra-coronavirus[.]com
- corona-armored[.]com
- corona-crisis[.]com
- corona-emergency[.]com
- corona-explained[.]com
- corona-iran[.]com
- corona-ratgeber[.]com
- coronadatabase[.]com
- coronadeathpool[.]com
- coronadetect[.]com
- coronadetection[.]com

2) MALICIOUS EMAIL SUBJECTS:

- RE: COVID-19 UPDATE
- Covid-19 in the Workplace: The Malaysian Position
- Update: Cruise ship outbreak of COVID-19 (Feb 17 2020)
- India,Äôs world power ambitions without hard power; Modi disappoints Western Liberals & Conservatives; Pakistan-Malaysia ties; and Pakistan,Äôs response to Coronavirus
- Coronavirus Updates
- Coronavirus - How to protect against it
- Update on Coronavirus

- March General Meeting (Covid-19)
- Coronavirus advisory information - Alert!! and Health Warning.
- Cloud Solutions for Supporting Your Business in Fighting the Coronavirus
- Urgent Information COVID-19 (Coronavirus) Update for your safety.
- TAKLIMAT JANGKITAN COVID-19 ‚Äì WARGA AWAM KEMENTERIAN PERTAHANAN
- FW: Coronavirus (2019-nCoV)
- Coronavirus (2019-nCoV)

3) MALICIOUS FILE/URL HASHES:

- 273b7f3b24448da30b50ebd61de76be2
- a81bae4c1d10bc011b6caf8c93268e40
- 1435fb770b222c3b4e1bd1b1addf1fa3
- fb3db3f1ea731ea53b2aacd55440d8cc
- f241a4e610db2e5bec54bc9a93bb60b8
- ef9d87523920688b81fea2d0705cef7d
- ebddf3d9b96ee88ec63ef750c2c81b2b
- ea1905b70f1b33b41e65f0bf6336e96c
- e6a2830946667f4d819a9ee12a03c292
- dfa006254bc6ad7c37e0456dfbb0145a
- de04d3027ee98658dcfdbcd7e60e0ffb
- da8b8afc896874fbf6ffb1aa966a61d4
- d986a0542f155609d48a8235d28b579d
- d5ecf471e81fcba8e5e098e06b1ab595
- d365c0591d4675b89db585315ff2b33c
- d314e98d60c542876f5201ab003a8063
- d05fba70c04316356f4d990901c11148
- ccfc1496385d320a8b90c1ccc0e5f554
- c88cec167226e9d0be4c89218710fd93
- c5d549357aef830e6048ce4117ee71e7
- c274b0c673d9f6e5eab50ba8c48340f5
- c04c9adfb986827864fb87adc1dfbab4
- bd1c50848d07f7ad806a02ebe63167d6
- b9c729eaefe1a88049de01fa5479c670
- ad604829e5d4b8b7054dc84d230e31a4
- acd9f964eaafc5472546228e0ea55875
- aca3a26ac98e06d3b288efeaefa64b38
- ab47342bb9beaae590d57ccf42f7a107
- a1e4d49195c619e8b7e12b02b8c5eb13

- 9bdb881ddfc1f443ed076e9f3c85f901
- 98e65d8c85b262b3e29806fe9966140d
- 97618422968b64b8c578d83d02a4bd82
- 96264606f3e15144a885d21fa65e624f
- 94cf6045791964dcabcb04cfa773294d
- 895e574906330814be676dab3c60eaf3
- 859aa54b44a3ce3477ff473facdfdafb
- 78fd215bc0b5172e9440025309965d73
- 78306edb61fd6147271a3005ef5ce5dc
- 6ca36c7c1488a795ed554088391bf614
- 66dab0bed444592f95027e6cb44a5154
- 65b469b74c007eaacd3bba5f90862a19
- 5d8a538f9c5735c7f2731d359e719a67
- 5c5ed3502a9ecca14e0fbdd86cb0ba56
- 56a089a2e6231b8f79fa8563809f722a
- 517a10f5e216bcac7fcff25709b2be2c
- 4e2f8e9206a86576d7ebbbb3ae66a4fb
- 48e2399523c850780ba95e7011365e83
- 3a0a3b5c4a8e7b130d1979454cd22bb3
- 30577f0aefb19790e401b67110d7ee48
- 23008ee5dfa9fa64272e9f0ec233c7ee
- 1f857fdadce1521833d338be656ae578
- 128fc88aa0b8691793496ce15f8e8dc7
- 11becee8e48e7ab93aec7ccaca505eca
- 0d44aed754d0e3f6a56c3b8152743803
- 09185936ac116c87017538a7f0f07449

Beware of Malicious Android App Being Distributed Through A Fraudulent Website Claiming to Be from The Perdana Menteri Malaysia

Introduction:

The National Cyber Security Agency (NACSA), National Security Council (NSC) through the National Cyber Coordination and Command Centre (NC4) has been informed of a malicious Android mobile app and a fraudulent website (http://malaysiagovermentapp.com) claiming to be from the Perdana Menteri Malaysia for the purposes of COVID-19 aid programme.

Impact:

Identity theft and financial loss.

Brief Description:

From our analysis, the malicious Android app is being used to trick victims into submitting their internet banking details, which will then be uploaded to a different website. It is observed that the Android app also has the capability to read mobile phone SMSes, which may be used to steal victim online banking credentials and TAC codes for Internet banking.

Recommendation:

The NC4 would like to remind the public to not access or install any suspicious links or applications that are not in the Google Play Store or the Manufacturer's App Stores such Apple AppStore, Huawei AppGallery, and Samsung Galaxy Store. It is also advised for the public to take the following actions:

1. DO NOT click on any links from unsolicited SMSes;
2. If you have clicked on the link, DO NOT download the Android app;
3. Make sure to download any apps from the official Google Play Store or Manufacturers' App Store;
4. Any official SMS sent by MKN on COVID-19 will be automatically tagged as "MKN" by the telco and doesn't provide any number for reply; and
5. Any official information and advisory regarding COVID-19 will be distributed ONLY on MKN official social media accounts as below
    a. Telegram : https://t.me/MKNRasmi
    b. Facebook : fb.me/MajlisKeselamatanNegara
    c. Twitter : https://twitter.com/mknjpm
    d. Website : https://www.mkn.gov.my

Appendix:

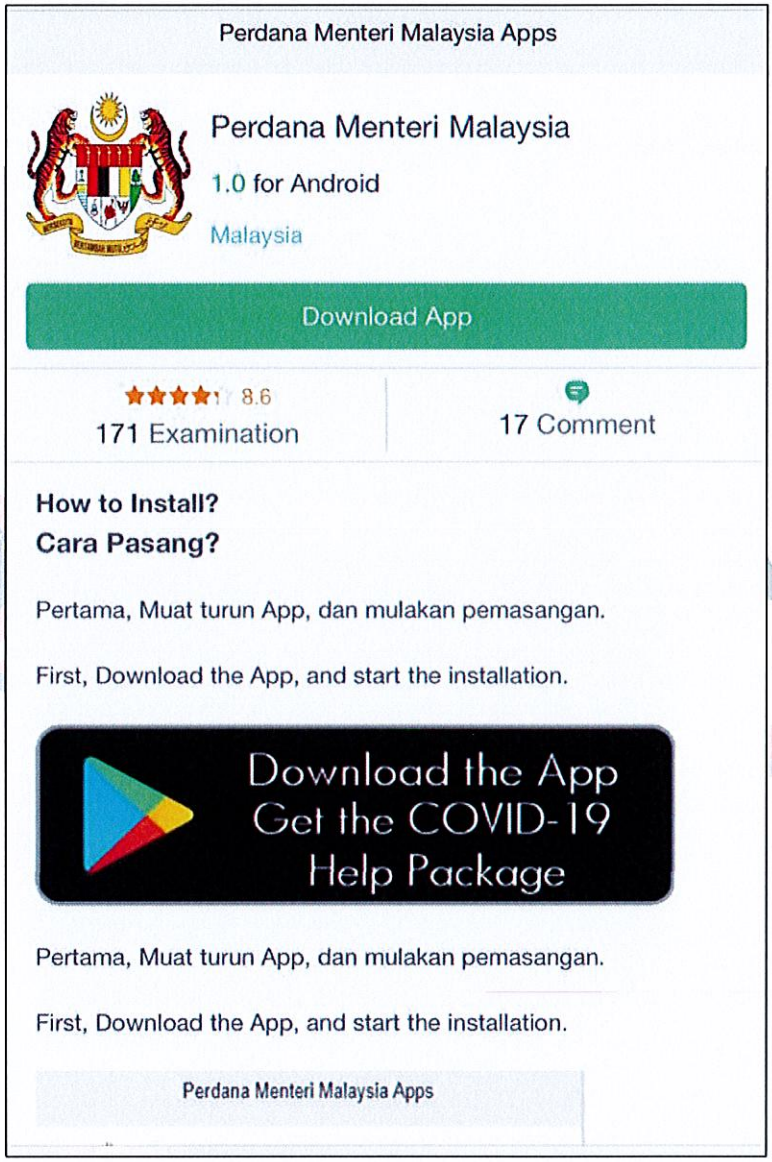

Figure 1: The fake website for the Android Malware.

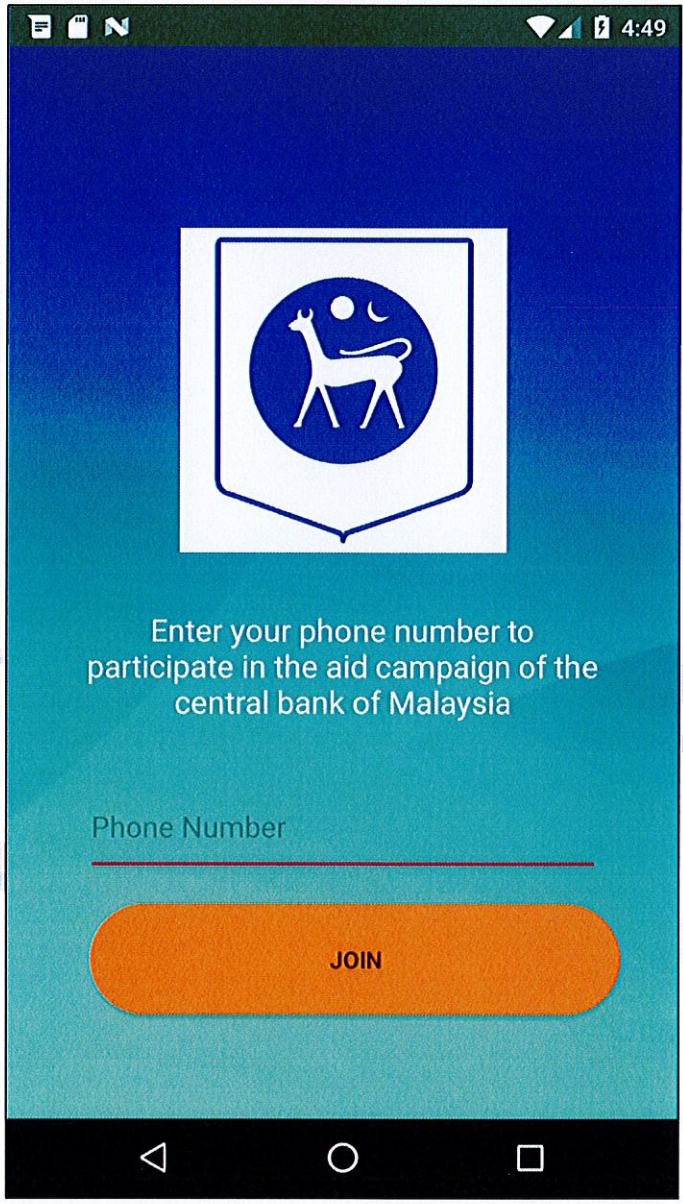

Figure 2: The Android Malware Main App

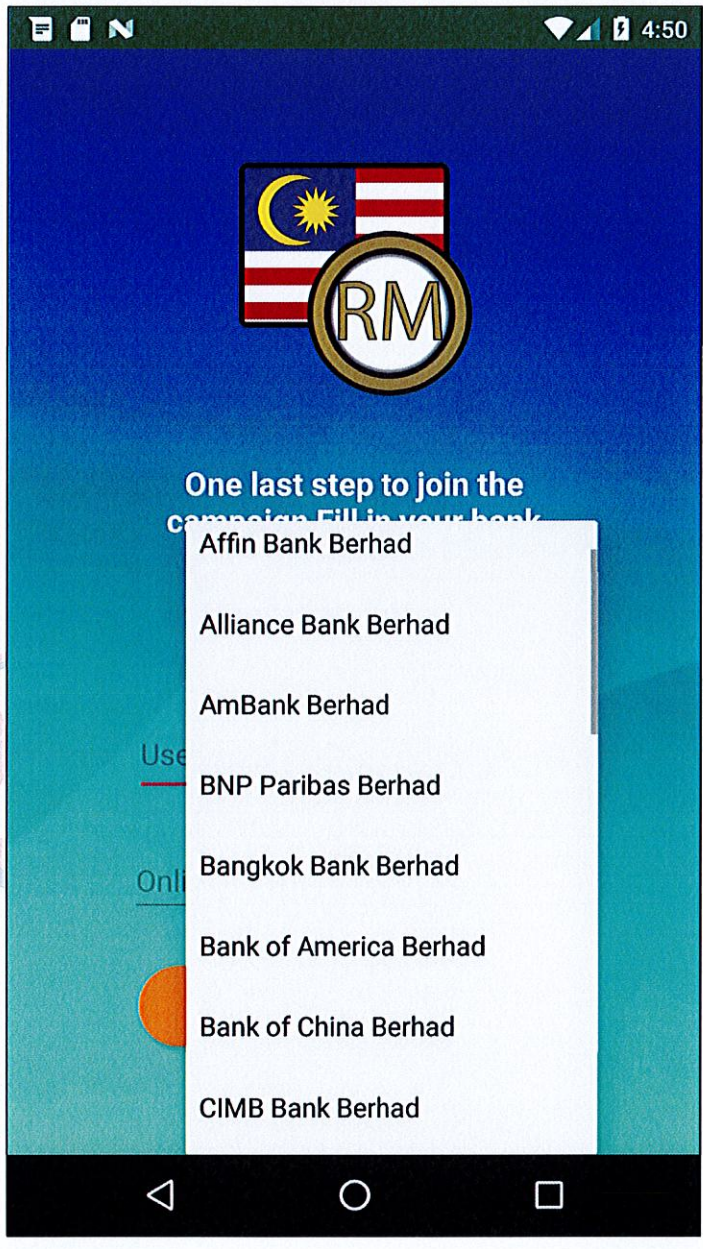

Figure 3: The Android Malware App Requesting Bank Info

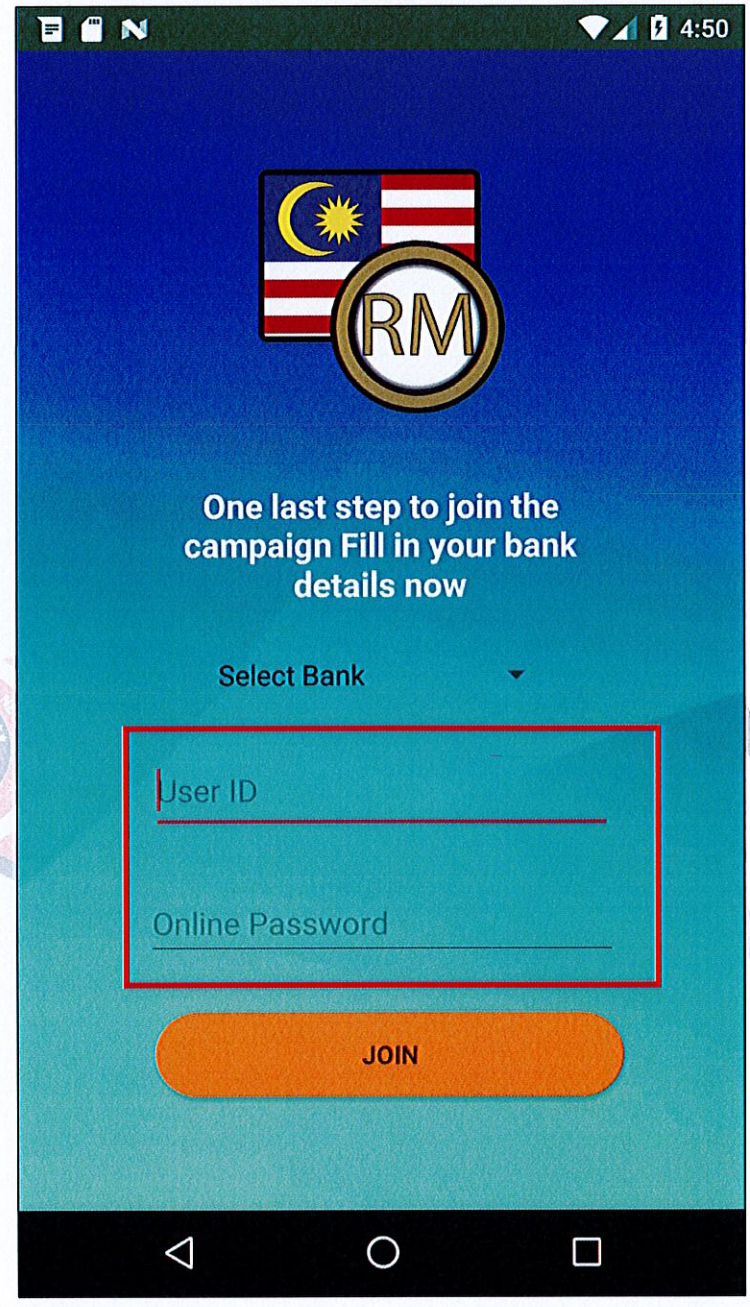

Figure 4: The Android Malware App Requesting Bank Credential