Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
Camp BGen Rafael T Crame, Quezon City

MEMORANDUM

NOTED SEP 0 6 2021
TCDS

FOR : See Distribution

FROM : D, ITMS

SUBJECT : **Cybersecurity Advisory | Project Pegasus**

DATE : September 02, 2021

---

1. References:
   a. Facebook Video Post of TV Patrol on August 26, 2021; and
   b. Website news article of CNN Philippines on July 20, 2021: https://www.cnnphilippines.com/business/2021/7/20/Pegasus-Project-journalist-spying.html.

2. Above references pertains to the "Project Pegasus" allegedly installing "Pegasus spyware" on their victims' mobile devices. Potential targets of Project Pegasus include journalists, human rights defenders, academics, lawyers, politicians, and several heads of state from different countries such as India, Mexico, Hungary, Morocco, and France, among others.

3. Pegasus spyware, also dubbed as one of the most advanced spyware, was created by NSO Group, an Israeli technology firm targeting criminals and terrorists. However, the said spyware has been widely misused and has instead victimized innocent personalities.

4. Like other spyware, Pegasus spyware can be installed remotely on one's mobile device without requiring any action from its owner. Once installed, it allows clients to take complete control of the device, including reading emails and messages, access GPS location, download or delete files, and turning on the camera and microphone.

5. Today, there have been no prior incidents of hacking using the Pegasus spyware recorded within the Philippines. However, numerous hacking incidents have been reported, such as the hacking of the vaccination registration website of Manila and the hacking of voters' data of COMELEC.

6. There are different ways on how a mobile device or a computer be infected with spyware, such as:
   a. Downloading illegal software from untrusted sources;
   b. Using public Wi-Fi from coffee shops and malls;

c. Clicking links commented by a follower or a friend from a social media post;

d. Downloading malicious apps from app stores;

e. Opening links from emails sent by unknown sender leading to a malicious website; and

f. Downloading and Opening infected files attached from emails disguised from a trusted source.

7. In this regard, this Service recommends the following security measures to be undertaken to avoid being a victim of spyware and other cybersecurity-related attacks:

a. Only download files from legitimate sources;

b. Refrain from clicking any random links sent or posted by unknown sources and friends;

c. Avoid downloading suspicious applications;

d. Do not open links or download email attachments from the unknown and unverified senders;

e. Regularly update your device's security through system updates; and

f. Invest in software security products such as antivirus and antimalware.

8. To learn more, you may visit https://itms.pnp.gov.ph to download learning materials under the Computer Security tab. Should you have inquiries and concerns, do not hesitate to call us at (02) 8723-0401/8537-4500 local 6546 or email us at issd.itms@pnp.gov.ph

9. For widest dissemination.

DANIEL C MAYONI
Police Brigadier General

Ali Amir Hassan Ramos

Distribution:
IG, IAS
DIPOs
D-Staff
P-Staff
D, NSUs
RD, PROs

Copy Furnished:
Command Group
SPA to the SILG