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

ITMS(IS)-230206-0005
MEMORANDUM

FOR : See Distribution

FROM : AD, ITMS

SUBJECT : **Cybersecurity Bulletin | Dark Pink APT Group**

DATE : February 6, 2023

---

1. References:
   a. Facebook post of Philippine National CERT dated January 12, 2023; and

   b. https://www.group-ib.com/blog/dark-pink-apt/.

2. The above references refer to recent cyber-attacks on government and military organizations, development agencies, religious organizations, and non-profit organizations in the Asia-Pacific Region by the newly discovered Advanced Persistent Threat (APT) Group, Dark Pink.

3. Dark Pink APT Group launched sophisticated cyber-attacks against the aforementioned organizations in Southeast Asia as early as mid-2021, and its first successful attack occurred in June 2022, when the group was able to access the network of a religious group in Vietnam. As of December 2022, the APT group had launched seven (7) successful attacks against ASEAN countries, including Cambodia, Indonesia, Malaysia, Vietnam, and the Philippines.

4. The APT group's attacks were typically launched with targeted spear-phishing emails, including one in which threat actors posed as a job seeker applying for an internship position. The phishing email contains custom malware that, once downloaded, can be used to exfiltrate data from their victims via Telegram, Dropbox, and email.

5. In light of the foregoing, this Service recommends the following steps to avoid becoming a victim of a cyber-attack:
   a. Be cautious when opening an email, especially from an unknown sender;

   b. Do not click on any suspicious links or download attachments from untrusted sources;

   c. Proactively monitor and secure identified systems and devices for any suspicious/malicious activities; and

d. Use anti-virus software and/or host-based detection tools running with the latest version to protect your data and devices.

6. You may visit itms.pnp.gov.ph to download learning materials regarding cybersecurity under the Computer Security Tab. Should you have any inquiries or concerns, you may contact ISSD at 8723-0401 local 6546 or e-mail us at issd.itms@pnp.gov.ph.

7. For widest dissemination.

JERICH T ROYALES
Police Colonel

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

Copy Furnished:
Command Group
SPA to the SILG