

1019

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad 4<sup>th</sup> July, 2022

Subject: - Cyber Security Advisory - New Malware/ Suspicious Appl "Nebula Shopping" (Advisory No. 24)

1. Introduction. A 3<sup>rd</sup> party application Nebula Shopping is targeting applicants/ users to acquire their personal and financial details such as mobile phone number, bank account and email ID; thereby making users vulnerable to identity theft and fraud. Such applications with other names can also be found on the web. Cyber probe and technical analysis against Nebula Application revealed that Nebula Shopping is allegedly a fraud application for earning money online and aims to provide easy loan through online order submission.

2. Recommendations

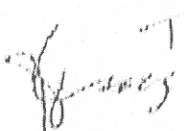
- 3912-  
7-7-22
- a. Don't Reveal Personal or Financial Information on 3<sup>rd</sup> Party apps. Do not respond to Application solicitation for this information.
  - b. Check security permissions of such apps before providing any sensitive information online.
  - c. In case, a user is not sure whether the app is legitimate, try to verify by contacting the company directly.
  - d. Block installation of apps from unknown sources, only install apps from official app stores, such as Google Play Store/ App Store.
  - e. Google Play protect (android built in Anti Malware) must not be switched off in any case as it detects suspicious apps in your mobile device based on their behavior and generates alerts.
  - f. Before installing any app, users must read its privacy policy explaining what data it is collecting from users and with whom it is sharing that data.
  - g. It is recommended that users should keep their communication app up-to-date from their respective App Stores. Do not ignore updates from apps installed on your device.
  - h. Regularly Update Mobile Operating System whenever updates are available.
  - i. Use Antivirus in order to prevent any danger that may compromise personal data stored on the device.
  - j. Carefully consider what information you want to store on the device, remember that with enough time, sophistication and access to the device, any attacker can obtain the stored information.

3. For any query or reporting malware, please forward the same on following email addresses: -

- a. eagle1978@mail.com
- 1600  
07-07-22
- 17/16
- 13-07-22
- Sy I a c.
- 7-7-22
- 07 JULY 2022

1750  
b. talcon098@writom.com  
c. asothab2@cabinet.gov.pk

4. Kindly disseminate the same message to all concerned in your organizations, all attached/ affiliated departments and ensure necessary protective measures.

  
(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph// 031-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

I-2