Pakistan Telecom Authority Headquarters, Islamabad

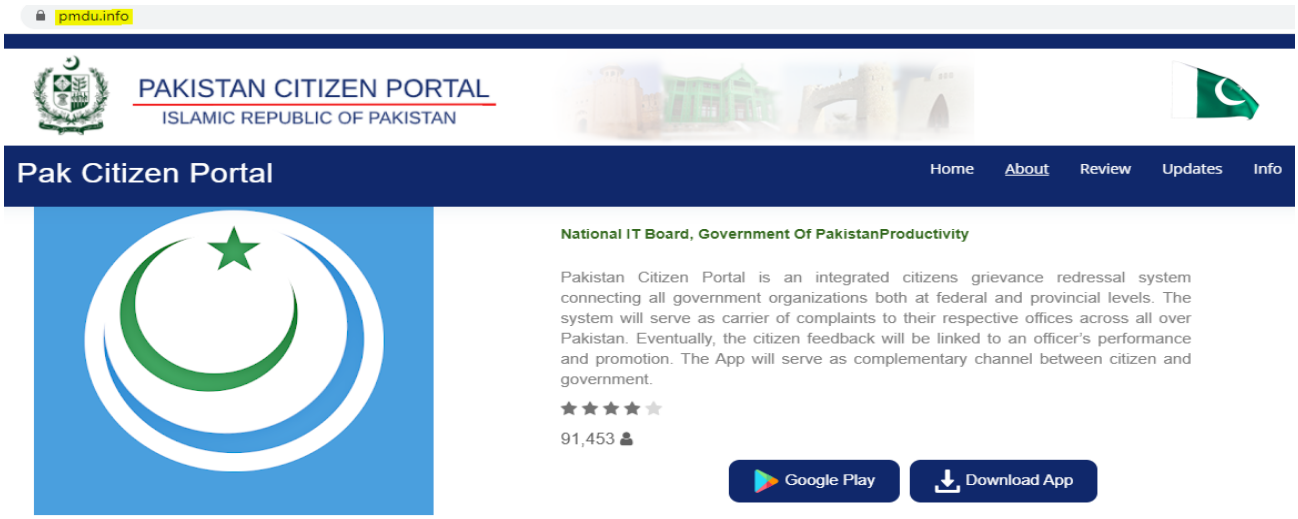
PTA Cyber Security Advisory No.:125 **15-01-2021**

Name: New Android spyware targeting users in Pakistan

Summary:

It has been recently reported that a cluster of **Trojanized** (malicious) version of Android apps are targeting Pakistani users for covert surveillance and cyber espionage. The modified apps look identical to their legitimate counterparts, and even perform their normal functions, but are designed to, initially, profile the phone, and then download a payload in the form of an Android Dalvik executable (DEX) file. It contains malicious features which may covertly exfiltrate sensitive data like the user's contact list and the full contents of SMS messages and then send such information to one of command-and-control websites hosted on servers located in eastern Europe.

The highest-profile app Trojanized is the Pakistan Citizen Portal app, which is hosted at website '**pmdu.info**' that appears to be a good mimicry of a Google Play Store page blended with elements from the legitimate Pakistan Citizen Portal page with **.gov.pk** domain. The malicious site is hosted on '**5.2.78.240'** IP address that geolocates to the **Netherlands**, which has been blocked by PTA, however, users accessing from abroad can become victim.



In addition, there are some other malicious versions of legitimate apps like a Muslim prayer-clock app called 'Pakistan Salat Time', 'Mobile Packages Pakistan', an app to check a phone's SIM card for validity called 'Registered SIMs Checker', maliciously modified version of the app published by TPL Insurance.

For further details including technical analysis, please visit following link:
https://news.sophos.com/en-us/2021/01/12/new-android-spyware-targets-users-in-pakistan/

Recommendations:

- Please disseminate to your subscribers.
- It is highly recommended that users should **only install apps from trusted sources** such as from government websites, or any official App / Play store.
- Always **review the App permissions** before/ after installation and disable unnecessary permissions especially camera, location, microphone, SMS etc. after installation).
- In settings, do not enable installation of apps from "UNTRUSTED SOURCES".
- Install, scan and update well reputed Anti-virus solution on all mobile devices.
- Do not download or click on links received from untrusted source via SMS/ Email/ WhatsApp and similar communication apps.
- Regularly provide Cyber security awareness sessions for employees and continuously arrange capacity building of the relevant technical resources.
- Do not download attachments from emails unless they are from the trusted source.
- In case of any incident, please report to this office.