Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 226 **02-02-2024**

Name: Patchwork Spyware Campaign Using Romance Scams

Threat Classification: State-Sponsored Espionage

Affected Software / Services:

- Android Apps (MeetMe, Let's Chat, Quick Chat, Rafaqat, Wave Chat, etc.)

Summary:

Suspected Indian state-sponsored hacking group, Patchwork, deployed at least 12 malicious Android apps through Google Play, targeting victims using romance scams. The APT group lured victims into downloading malicious apps, including messengers and a fake news app. Once installed, the VajraSpy malware got activated, enabling the exfiltration of sensitive data, such as contacts, SMS messages, call logs, device location, and files. Advanced functionalities included intercepting messages from apps like WhatsApp and Signal, recording phone calls, taking pictures, logging keystrokes, and scanning for Wi-Fi networks. Patchwork has a history of state-sponsored cyber-espionage activities.

Severity	**Critical**
Attack Vector	Network / Social Engineering

Recommendations:

- Regularly check app permissions and reviews before downloading applications, even from official stores.
- Use mobile security solutions to detect and prevent the installation of malicious apps.
- Educate users about the risks of romance scams and the importance of verifying the legitimacy of apps.
- Implement multi-factor authentication to add an extra layer of security to account logins.
- Stay informed about state-sponsored cyber threats and implement security measures accordingly.
- In case of suspected compromise, conduct thorough security audits and follow incident response protocols.
- In case of any incident, please report to this office, through PTA CERT Portal and email.