Severity

High

Analysis Summary

Donot APT group has been actively dropping malicious samples and targeting Government users to exfiltrate data. The group has previously been active in the past and has now again shifted its focus to phishing campaigns. The group has a history of attacking Pakistani government officials and military personnel and has been linked to India. They previously targeted Pakistani users with android malware named (StealJob) was used to target Pakistani android mobile users by Phishing on the name of “Kashmiri Voice” The attackers hunt for confidential information and intellectual property. The hackers’ targets include countries in South Asia, in particular, the state sector of Pakistan.

Impact

- Information Theft and Espionage

Indicators of Compromise

MD5

- 7e088808e52ed5eb88d4a2df6c77cfae

SHA-256

- 3342d74ec2b0c7324d6cc94a6e9989f002ec02b43927fe6b0951e160829843be

SHA-1

- c43241f4e342dfac9bf3c119e3792b937409fe06

Remediation

- Block the threat indicators at their respective controls.
- Search for IOCs in your environment.