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

- 3e6cf707c43ee31a42a17d70e8e8cab3

SHA-256

- 8eb9e93adb4e5e6bf5fac0d0b9de5897aa7274ef451b84854a0da38db61a502a

SHA-1

- 28f28b23b137a04a1d45dea89d67e815169a998e

Remediation

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