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

- 2b8a240bde4644ed045ccda1dd2a36b6
- 350204a366fd3a2b1b9b80e6891c0df3
- 8b2c183f32e0dd20856d1661d732f614

SHA-256

- 15e2a10772575e77d1041394191a4db7a665da96889346da0d2e7b6a3aa455b3
- 7952c02ea6c90e29370ee0e80b754156a2e5b1f473b2a469fdde3426a20e9356
- 635ad590116dc390141f58b4dded72d9d6d51d83c10cb60ca6e0d7e00b1ef4d4

SHA-1

- ea70cc9a587fe2634669251f578ab4b9a29374f3
- 5a2a1f68dc7d11cd330d1584e75febef19813d2e
- 6ce8819d2b385568bf5eccc24e079ba301461bd8

URL

- https[:]//kokoo[.]live/D7yrtjdcjjd3jjw2jdj7vvNsso0oR/5trT0o0oOO0retnRKKLmM
- http[:]//log[.]bookservices[.]xyz/

Remediation

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