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

Domain Name

- records[.]hibiscus[.]live

MD5

- 17efa6a9b3547aaad4588c07f9773e6a
- a2b3599d36c2ab1317b4560931f689cb

SHA-256

- 9c03bd3791da05df6d7c18cebfa55fd156edb12ff41845336803ae3ee540b96d
- 5b6c10c35cab002750ba16aa8eba4f46d8e7267ae7c40c9e610add6da01ba3fd

SHA-1

- 05c62ac69f88d5bbffc2b3c187ff0c9c8d20664c
- a77859e2c34d890d3e0ca76400264ac14c9da723

URL

- http[:]//records[.]hibiscus[.]live/NDnD7RdekyhSrhPE/KOighzucGWiCq6hR[.]php

Remediation

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