On Information Security Incident of March 10, 2018

- ISRO received an alert about a Trojan (XtremeRAT) in one of the ISRO Units, "ISRO Telemetry, Tracking and Command Network (ISTRAC)." **Subsequent analysis revealed that it was a false positive** i.e. a software detected an issue which was actually not present.
    - It mentioned a victim IP address/ Port infected with XtremeRAT. However, this was a UTM Port, not mapped internally to any systems (no internal system was associated with that IP address/ Port). This Port was meant for login service (with Multi factor Authentication) for specific employees of the organization.
    - Nevertheless, the reported Port was disabled as a precautionary measure and later the same service was enabled through an alternate mechanism.
- The alert was based on output of a search done on a third party website (for that particular IP address of ISTRAC), which wrongly listed ISTRAC IP/ Port as infected with XtremeRAT.
- After investigation, it was concluded that there was no infection of XtremeRAT on ISTRAC systems and the reported incident was a **false alert**.

Note:

- Mission Critical systems in ISTRAC are not connected to Internet.
- ISRO is considering a separate mechanism for responsible disclosure of cyber security incidents such that inputs are directly accessible to IT team.
- ISRO appreciates security researchers for responsible disclosure and their efforts, within the ambit of applicable legal framework.

****