Hermit spyware

June 30, 2022

In news– Hermit spyware is believed to have targeted iPhone and Android devices in Italy and Kazakhstan.

What is Hermit spyware?

- Hermit is a spyware on the lines of Pegasus by NSO Group and **developed by an Italian vendor called RCS Lab** and was **first reported by cyber security researchers at the Lookout,** a San-Francisco-based cybersecurity firm.
- **Once installed on a device, it can record audio on the device**, **carry out unauthorised calls**, and carry out many unauthorised activities.
- It can s**teal stored account emails, contacts, browser bookmarks/searches, calendar events**, etc.
- **It can also take pictures on the device**, steal device information such as details about applications, the kernel information, model, manufacturer, OS, security patch, phone number, etc.
- It **can also download and install APK** (the app software files on Android) on a compromised phone.
- The spyware **can also upload files from the device, read notifications,** and take pictures of the screen.
- It **can gain access to the root or the 'privilege' access of an Android system,** and it can **uninstall apps like Telegram and WhatsApp**.
- It can also steal data from the old app.
- For WhatsApp, it can prompt the user to reinstall WhatsApp via Play Store.

How did they get past both Apple and Google's security measures?

- The actors targeting the victims had to **work with the target's 'Internet Service Provider' or ISP** to disable the target's mobile data connectivity.

- **Once disabled, the attacker would send a malicious link via SMS asking the target to install an application** to recover their data connectivity.
- **When ISP involvement was not possible, the spyware would pretend to be a messaging app.**
- The link would pretend to be a recovery page for a Facebook account and ask users to download a version of either WhatsApp, Instagram or Facebook.
- **In Apple's case, Google's research showed that the spyware exploited Apple's enterprise certificate,** which is given to apps by select enterprises.
- This certification allows companies to distribute their own in-house apps for direct downloads on iOS devices, bypassing the App Store.
- The 'Hermit spyware' apps had managed to get these certifications, which have since been revoked by Apple.