Sova malware

September 20, 2022

In news– The new mobile banking 'Trojan' virus – SOVA – which **can stealthily encrypt an Android phone for ransom** and is **hard to uninstall** is targeting Indian customers.

About SOVA-

- It **can add false overlays to a range of apps and "mimic" over 200 banking and payment applications** in order to con the Android user.
- The **latest version of this malware hides itself within fake Android applications** that show up with the logo of a few famous legitimate apps like Chrome, Amazon, NFT (non-fungible token linked to crypto currency) platform to deceive users into installing them.
- The lethality of the virus can be gauged from the fact that **it can collect keystrokes, steal cookies, intercept multi-factor authentication (MFA) tokens,** take screenshots and record video from a webcam and can perform gestures like screen click, swipe etc. using android accessibility service.
- It is the refactoring of its "protections" module, which aims to protect itself from different victim actions.
- For example, **if the user tries to uninstall the malware from the settings or pressing the icon, SOVA is able to intercept these actions** and prevent them by returning to the home screen and showing a toast (small popup) displaying "This app is secured".
- It can **jeopardise the privacy and security of sensitive customer data** and result in "large-scale" attacks and financial frauds.
- **It was earlier focusing on countries like the US, Russia and Spain,** but in July 2022 it added several other countries, including India, to its list of targets.
- **India's federal cyber security agency(CERT-In) issued an**

advisory saying that the virus has upgraded to its fifth version after it was first detected in the Indian cyberspace in July.

- **The first version of this malware appeared for sale in underground markets in September 2021** with the ability to harvest user names and passwords via key logging, stealing cookies and adding false overlays to a range of apps.

How does it work?

- As per CERT In, **once the fake android application is installed on the phone,** it sends the list of all applications installed on the device to the C2 (command and control server) controlled by the threat actor in order to obtain the list of targeted applications.
- At this point, the C2 sends back to the malware the list of addresses for each targeted application and stores this information inside an XML file.
- These targeted applications are then managed through the communications between the malware and the C2.

The Indian Computer Emergency Response Team or CERT-In-

- It is an office within the Ministry of Electronics and Information Technology of the Government of India.
- It is the nodal agency to deal with cyber security threats like hacking and phishing.
- It strengthens security-related defence of the Indian Internet domain.
- CERT-IN was formed in 2004 by the Government of India under Information Technology Act, 2000 Section (70B) under the Ministry of Communications and Information Technology.
- It has overlapping on responsibilities with other agencies such as National Critical Information Infrastructure Protection Centre (NCIIPC) which is under the National Technical Research Organisation (NTRO) that

comes under Prime Minister’s Office and National Disaster Management Authority (NDMA) which is under Ministry of Home Affairs..