SOVA Android Trojan targets Indian Banking customers

- SOVA Malware initially detected in September 2021 which was earlier reported to target East European countries, has added India also to its target list.
- The malware hides itself within fake Android applications that show up with the logo of legitimate apps like Chrome, Amazon, etc.
- The new version of SOVA is targeting more than 200 mobile applications including banking apps and crypto exchanges/ wallets. It also shows code development including ransomware feautures.
- The SOVA malware’s list of functions includes the ability to collect keystrokes, steal cookies, intercept multi-factor authentication (MFA) tokens, take screenshots and record video from a webcam, perform gestures like screen click, swipe, etc. using the android accessibility service, copy/paste, adding false overlays to a range of apps, mimic over 200 banking and payment applications.

Best Practices and recommendations

Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device’s manufacturer or operating system app store.

Prior to downloading / installing apps on android devices (even from Google Play Store):
- Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
- Verify app permissions and grant only those permissions which have relevant context for the app’s purpose.
- Do not check "Untrusted Sources" checkbox to install side loaded apps.

Install Android updates and patches as and when available from Android device vendors.

Do not browse un-trusted websites or follow un-trusted links and exercise caution while clicking on the link provided in any unsolicited emails and SMSs.

Look for suspicious numbers that don’t look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number.

Do extensive research before clicking on link provided in the message

Exercise caution towards shortened URLs

Report to hoisg@canarabank.com or ciso@canarabank.com in case of any incidents

A V RAMA RAO
Chief General Manager

Ref: SOVA Android Trojan Alert by CERT-In (https://www.csk.gov.in/alerts/SOVA.html)