SOVA Android Trojan Targets Banking Customers

Capabilities:

- 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 android accessibility service
- Copy/paste
- Adding false overlays to a range of apps
- Mimic over 200 banking and payment applications

- SOVA Android Trojan is a new type of mobile banking malware. First version of this malware appeared for sale in underground markets in September 2021
- SOVA has the ability to harvest usernames and passwords via key-logging, stealing cookies and adding false overlays to a range of apps. New version of SOVA is capable of hiding itself within fake Android applications that show up with the logo of a few common legitimate apps like Chrome, Amazon, and NFT platform to deceive users into installing them.
- SOVA seems to be targeting more than 200 mobile applications, including Banking Apps and Crypto exchanges/wallets. Moreover its latest version shows various code development including Ransomware features. AES encryption technique is used to encrypt files on infected device and ".enc" extension is appended to the infected file name.

MODUS OPERANDI:

- Malware is distributed via smishing (phishing via SMS) attacks, like most Android banking Trojan

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
- Exercise caution while clicking on the link provided in any unsolicited emails and SMS.
- Do extensive research before clicking on link provided in the message. There are many websites that allow anyone to run search based on a phone number and see any relatable information about whether or not a number is legit.
- Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organisation's website directly using search engines to ensure that the websites they visited are legitimate.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Exercise caution towards shortened URLs, such as those involving bit.ly and tinyurl.
- Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information such as personal particulars or account login details.