SOVA Android Trojan

It is reported that Indian banking customers are being targeted by a new type of mobile banking malware campaign using SOVA Android Trojan. The first version of this malware appeared for sale in underground markets in September 2021 with the ability to harvest usernames and passwords via keylogging, stealing cookies and adding false overlays to a range of apps. SOVA was earlier focusing on countries like the USA, Russia and Spain, but in July 2022 it added several other countries, including India, to its list of targets. 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 platform to deceive users into installing them. This malware captures the credentials when users log into their net banking apps and access bank accounts. The new version of 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.

Infection Mechanism

As observed, the malware is distributed via smishing (phishing via SMS) attacks, like most Android banking Trojans. 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 malware is capable to perform the following functions:

- 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

It has been discovered that the makers of SOVA recently upgraded it to its fifth version since its inception, and this version has the capability to encrypt all data on an Android phone and hold it to ransom. Another key features of SOVA is the refactoring of its "protections" module, which aims to protect itself from different victim’s 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 (through the abuse of the Accessibilities) by returning to the home screen and showing a toast (small popup) displaying "This app is secured".

These attack campaigns can effectively jeopardize the privacy and security of sensitive customer data and result in large scale attacks and financial frauds.

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.
- Install and maintain updated anti-virus and antispyware software.
- 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. Genuine SMS messages received from banks usually contain sender id (consisting of bank's short name) instead of a phone number in sender information field.
- 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. Users are advised to hover their cursors over the shortened URLs (if possible) to see the full website domain which they are visiting or use a URL checker that will allow the user to enter a short URL and view the full URL. Users can also use the shortening service preview feature to see a preview of the full URL.
- 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.
- Customer should report any unusual activity in their account immediately to the bank with the relevant details for taking further appropriate actions.