बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

CISO CELL
Head Office, Pune - 411005

Dear Valued Customer,

17/09/2022

Thank you for banking with Bank of Maharashtra!

Security of your account is of utmost importance to us. In our endeavour to continue educating our customers on security, we are hereby publishing the Customer Awareness Series - 37. Please find the same below. Hope you will find it useful and informative.

Customer Awareness – 37
SOVA Android Malware

Indian banking customers are being targeted by a new type of mobile banking malware campaign using SOVA Android Trojan. 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.

Infection Mechanism

The malware is distributed via smishing (phishing via SMS) attacks, like Android App. Once the fake android app is installed on the mobile phone, it sends/ captures the list of all applications installed on the device and targets specific financial applications.

The malware is capable 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 android accessibility service, copy/paste, and even mimic over 200 banking and payment applications. The malware also has the capability to encrypt all data on an Android phone and hold it to ransom.

The malware is also capable to protect itself from victim's activities, e.g. 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 pop up - displaying "This app is secured".

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 (like Google Play store).
- Prior to downloading / installing apps on android devices (even from Google Play Store):
  - o Always review the app details, number of downloads, user reviews, comments and "ADDITIONAL INFORMATION" section.
  - o Verify app permissions and grant only those permissions which have relevant context for the app's purpose.
  - o 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.
- Take sufficient precautions 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 tiny-url. 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 respective bank with the relevant details for taking further appropriate actions.
- Change the passwords of Financial Applications regularly and don't save on device.
- Turn on internet data, only whenever required (specifically Turn Off data during night time).
- Monitor the data usage for any unusual activity.

Such attacks effectively jeopardize the privacy and security of sensitive customer data and result in largescale attacks and financial frauds. Branches are advised to take necessary precautions against any such malwares and always follow best practices

- Chief Information Security Officer,
Bank of Maharashtra