केनरा बैंक Canara Bank
सिंडिकेट Syndicate

Beware of Drinik Android Malware

Targeting Indian Banking customers

WHAT IS DRINIK MALWARE?

- Drinik is a malware which is targeting Indian taxpayers to steal customer Personal Identifiable Information (PII) and banking credentials through Phishing attacks.

FEATURES OF DRINIK MALWARE

- In the latest version the Drinik malware appears in the form of an Android Package Kit (APK) called iAssist.
- The malware has transformed into an Android Trojan that may steal sensitive information such as banking passwords and personal information.

WHAT CAN DRINIK MALWARE DO?

- Using call Screening Service to block incoming calls
- Abusing accessibility
- Screen recording to retrieve credentials
- Keylogging
- Stealing credentials from genuine websites
- Receiving commands through Firebase Cloud Messaging
- Overlay attack to get permission for performing desired function without the customer's knowledge etc.

HOW DOES MALWARE TRAP CUSTOMERS?

- The newly-upgraded Drinik Malware loads the actual page of the Income Tax department rather than a fake phishing page.
- The website displays a biometric authentication screen rather than the login page. Once the victim enters the pin, the malware would steal it using the screen recording feature. It can also capture keystrokes to get the credentials.
- Further, malware steals victim's user ID (Aadhar Card, PAN Card, etc.)
- It further opens a dashboard on the genuine website, displaying the following fabricated message:

> ***"Our database indicates that you are eligible for an instant tax refund of Rs.57,100.\ from your previous tax miscalculations till date. Click Apply to apply for instant refund and receive your refund in your registered bank account in minutes."***

- The victim is persuaded to select the 'Click Apply' option and verify sensitive information which is later misused by hackers.

HOW TO PREVENT GETTING COMPROMISED?

- Download and install software only from official app stores like Play Store or the iOS App Store.
- Never share your Card Details, CVV number, Card PIN, and Net Banking Credentials with an untrusted source.
- Be cautious of opening any links received via SMS or emails delivered to your phone.

READ MORE CYBER SECURITY TIPS AT:
https://canarabank.com/User_page.aspx?othlink=356