Drinik Malware

An upgraded version of Drinik malware has been discovered that puts data of customers at risk. According to analysts, the malware has evolved into an Android Trojan that can steal important personal details and banking credentials. It was operated as an SMS stealer, but has now added banking Trojan features. In the new form, it is capable of screen recording, keylogging, abusing Accessibility services, and performing overlay attacks.

How does the Drinik Android trojan target customers?

As per the report, the latest version of Drinik malware comes in the form of an APK named iAssist. The iAssist is the official tax management tool of the India Tax department. Once installed on a device, the APK file will ask for permission to read, receive and send SMS in addition to reading the user's call log. It also requests permission to read and write to external storage.

Similar to other banking Trojans, Drinik relies on Accessibility Service. After launching, the malware prompts the victim to grant permissions, followed by a request to enable Accessibility Service. It then disables Google Play Protect and starts executing auto-gestures and capturing key presses.

Next, it loads the genuine Indian income tax site, instead of displaying fake phishing pages. Before showing the login page to the victim, the malware will display an authentication screen for biometric verification. When the victim enters a PIN, the malware steals the biometric PIN by recording the screen using MediaProjection and also captures keystrokes. The stolen details are then sent to the C&C server.

What is worrisome is that in the latest version of Drinik, the TA only targets victims with legitimate income tax site accounts. Once the victim logs into the account successfully, it shows a fake dialogue box on the screen mentioning the below message:

Our database indicates that you are eligible for an instant tax refund of ₹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.

It is here when the user is redirected to a phishing website when he clicks on the Apply button. The malware now prompts the victim to submit personal details such as full name, Aadhar number, PAN number, and other details along with financial information, which includes Account number, Credit card number, CVV, and PIN. The stolen data is again sent to the C&C servers.

Drinik targeting banks

Drinik Trojan malware targets banks using the Accessibility Service for events related to the targeted banking apps, such as their apps. Drinik abuses the "CallScreeningService" to disable incoming calls to interrupt the login and steal data.

How to stay safe from Drinik malware?

1. Download and install apps from Play Store only.

2. Enable biometric authentication security on apps and for the lock screen.

3. Never click on a link you receive from a random number or source.

4. Use Google Play Protect to check your apps and devices for harmful behaviour.

Google Play Protect is on by default, but you can turn it off. For security, we recommend that you always keep Google Play Protect on.

I. Open the Google Play Store app Google Play.
II. At the top right, tap the profile icon.
III. Tap Play Protect and then Settings.
IV. Turn Scan apps with Play Protect on or off.

5. Change app permissions on your Android phone:

You can allow some apps to use various features on your phone, such as your camera or contacts list. An app will send a notification to ask for permission to use features on your phone, which you can Allow or Deny. You can also change permissions for a single app or by permission type in your phone's Settings.