ADVISORY ON MALICIOUS GOOGLE PLAY STORE PAGES / APPLICATIONS

This is to bring to your kind attention that the large-scale scam campaign targeting users of Indian financial organizations through malicious Google Play Store download pages and fake applications (APKs) has been observed wherein malicious pages & applications are being used for harvesting banking credentials, monitor clipboard activities, log keystrokes, extracting contact information etc. In this connection, the brief overview of the campaign, lOCs, Domains, C2C Server URLs and the recommended actions are provided below:

Overview:

It has observed that a large-scale scam campaign targeting users of Indian financial organizations through malicious Google Play Store download pages. This operation involves meticulously crafted fake Play Store websites that closely mimic the official platform, successfully deceiving victims into downloading seemingly legitimate applications. However, the APKs obtained from these sources are actually Trojan malware designed to steal sensitive user information. Once installed, these malicious applications can harvest banking credentials, monitor clipboard activity, log keystrokes, and extract contact lists allowing attackers to exploit victims' personal and financial data for further malicious activities. The scale and complexity of this operation indicate a highly coordinated effort to compromise users globally.

Attack Vector:

Threat actors behind this scam register domain names that closely resemble those of trusted entities, mimicking official Google Play Store pages to deceive victims into downloading malicious apps. These threat actors also create fake APKs that appear similar to legitimate apps in both icon and name but are actually Trojans designed to act as spyware. The malicious APK is specifically designed to target devices running Android versions between 7.0 (SDK 24) and 13.0 (SDK 33). These malicious apps request dangerous permissions, including access to accessibility services, which enables the malware to capture screen content, monitor keystrokes for sensitive data like login credentials and private keys, and continuously track clipboard contents to steal cryptocurrency addresses or passwords, all without requiring explicit user permission.

Additionally, the malware targets a specific list of banks by searching for banking apps on the infected device. It then sends a complete list of installed applications to the attacker's server, checks for any apps from the target bank list, and waits for the right opportunity to steal the user's credentials.

The APK's list of functions includes the ability to:

- Credential Theft & Account Takeover — The Trojan may log keystrokes, capture credentials, or use phishing overlays to steal login details for banking apps, cryptocurrency wallets, or online payment platforms.
- Personal Data Harvesting — Scammers collect personal information such as names, addresses, phone numbers, and emails, which can be used for identity theft, social engineering attacks, or sold to third parties for targeted scams and fraud.
- SMS & MFA Interception — Some Trojans can intercept SMS messages, including one-time passwords (OTPs) sent by banks and services for multi-factor authentication (MFA). This allows attackers to bypass security measures and gain full control over compromised accounts.
- Ad Fraud & Botnet Operations — The malware may silently run in the background, clicking ads, generating fake traffic, or subscribing victims to premium services without their consent. In some cases, infected devices are recruited into botnets for large-scale fraud campaigns.
- Ransom & Extortion — Advanced malware variants can lock the victim's device, encrypt files, or threaten to leak sensitive data unless a ransom is paid.

Best Practices

1. 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.
2. 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.
3. Install Android updates and patches as and when available from Android device vendors.
4. 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.
5. 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.
6. 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.
7. Only click on URLs that clearly indicate the website domain. When in doubt, users can search for the organization's website directly using search engines to ensure that the websites they visited are legitimate.
8. Install and maintain updated anti-virus and antispyware software.
9. Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
10. 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.
11. 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.
12. Education and awareness program for cyber security awareness is suggested.
13. Customer should report any unusual activity in their account immediately to the respective bank with the relevant details for taking further appropriate actions.

*****