NCA-21.102524 – National CERT Advisory: Hostile APTs Targeting Pakistani Officials with Android Apps for Data Exfiltration

Introduction

Recent intelligence from National CERT has identified several suspicious Android applications on the Google Play Store that are believed to be part of a campaign targeting Pakistani officials. These applications are designed to extract personal and financial data, including media files, contact lists, calendars, and call/message logs from victims' mobile phones upon downloading—often without user consent. Some of these apps are even reported to offer personal identifiable information (PII) of Pakistani citizens for monetary exchange. This advisory outlines the technical details of the threat, key indicators of compromise (IOCs), and recommended security measures to safeguard users.

Campaign Details

The threat originates from malicious Android applications that masquerade as legitimate tools. Once downloaded, these apps silently extract sensitive information from users' devices. Key findings include:

- **Malicious Application Behavior:** Users who download these applications may unknowingly grant permissions that allow the apps to access sensitive data on their devices.
- **Data Exfiltration:** Upon installation, these apps collect personal and financial data, potentially leading to identity theft and financial fraud.
- **Targeted Information Offering:** Some of these applications claim to provide PII on demand, further exploiting user data for illicit purposes.

Indicators of Compromise (IOCs)

Suspicious Android Applications:

Sr. #	Application Name	Developer Info
2	Initial Test Preparation	ITAppCoding(itappcoding28@gmail.com)
3	Intelligence Mcqs Test	ITAppCoding
4	Pak eServices 2024	ITAppCoding
5	Electricity Bill Checker	ITAppCoding
6	Sui Gas Bill Viewer	ITAppCoding
7	Online Shopping Pakistan	ITAppCoding
8	All Sim Packages	ITAppCoding
9	Bike Services	ITAppCoding

Recommendations and Action Items

1. **Prevention Measures**
    a. **User Education:** Inform users about the risks associated with downloading applications from unknown developers and the importance of checking app permissions.
    b. **Application Installation:** Ensure that users only install applications from trusted sources (e.g., Google Play Store) and avoid third-party hosting sites.
    c. **Permission Management:** Regularly review and manage app permissions to ensure that no unnecessary access is granted.
    d. **Privacy Policy Review:** Users must read privacy policies before installation to understand what data is collected and how it is used.
    e. **Google Play Protect:** Do not disable Google Play Protect, the built-in antimalware feature on Android devices.
2. **Detection Measures**
    a. **Monitor App Behavior:** Encourage users to report any suspicious behavior from installed applications, such as unexpected data usage or prompts for excessive permissions.
3. **Incident Response and Mitigation**
    a. **Uninstall Suspicious Apps:** Advise users to immediately uninstall any applications from the list of suspicious apps and report them to National CERT.
    b. **Data Backup:** Regularly back up important data to prevent loss in case of a data breach.
4. **Best Practices**
    a. **Strong Passwords:** Encourage the use of strong passwords and multi-factor authentication wherever possible.
    b. **Antivirus Software:** Recommend the installation of reputable antivirus and anti-malware software, and ensure it is regularly updated.
    c. **Location Settings:** Advise users to keep location services turned off unless necessary, and avoid bringing smartphones into sensitive environments.

This advisory emphasizes the importance of vigilance when downloading applications and managing personal data on mobile devices. National CERT urges all officials and citizens to implement the security measures outlined in this advisory to protect against

these cyber threats. Regular monitoring and user education are essential in mitigating the risks associated with hostile APTs targeting Android users.