कर्मचारी भविष्य निधि संगठन
EMPLOYEES' PROVIDENT FUND ORGANISATION
(श्रम एवं रोजगार **मंत्रालय**, भारत सरकार)
(MINISTRY OF LABOUR & EMPLOYMENT, GOVT. OF INDIA)
राष्ट्रीय **डाटा केंद्र** / NATIONAL DATA CENTRE
1ST Floor, EPFO Complex, Plot No.23, Sector-23, Dwarka, New Delhi-110075
www.epfindia.gov.in

सत्यमेव जयते

Letter No: CISO/Security/2022/1401 Dated: 01/07/2022

Cyber Security Advisory No.2022/03: Protection against Mobile based Malware.

Reference: CERT-In Advisory CIAD-2022-0014 (May 30, 2022)

1. Availability of the smartphone and affordable high-speed mobile internet connection with people worldwide makes it a lucrative attack surface for cyber criminals. A variety of malwares are known to infect smart phones. Types of Mobile based malware are listed below:-

   a) **Adware** - Mobile adware is unwanted software designed to serve advertisements on your device. Some Adware also tracks user behaviour.

   b) **Cryptocurrency Mining Malware** - This type of malware uses device resources to perform complex calculations needed to generate cryptocurrency (cryptojacking).

   c) **Remote Access Tools** - These tools are used to access the device remotely and have complete control of the device like installed applications, call history, address books, web browsing history, SMS etc.

   d) **Mobile Banking Trojan** - These types of malware look like legitimate banking apps but aim to steal financial credentials and data on a targeted host.

   e) **SMS Trojan** - These Trojans use the SMS of a mobile device to send and intercept messages. The user is usually unaware of the behaviour.

   f) **Mobile Spyware** - A mobile spyware is a type of malware that records the action of users using mobile resources without the user's knowledge.

   g) **Mobile Ransomware** - These types of malware lock your mobile devices, make files on the device inaccessible or encrypts them unless a ransom is paid to the attacker.

2. **Countermeasures and Best practices for users are listed below:-**

a) **Keep OS and Apps updated** - Users should always check and ensure their mobile devices are running on the latest operating system (Android, iOS etc.). Users should enable auto-updating features for the operating system and mobile applications to get the latest security, privacy and flaw fixes.

b) **Use Strong Authentication** - Users should use strong login passwords and PINs and use biometric authentication (on supported devices). Also, users recommended to use two-factor authentication for apps that support them.

c) **Apply Mobile Application Security Measures** - Users are advised below measures for mobile application security.
   i. Use only curated app stores (Apple Store, Google Play Store) for downloading mobile applications.
   ii. Disable third-party app stores as they can be vectors for spreading malware.
   iii. Avoid installing apps from unknown sources
   iv. Periodically review mobile apps and delete applications which are not used or not needed.
   v. Minimise personally identifiable information (PII) data stored in apps.
   vi. Review Permissions required by each application critically and grant only those permissions which are utmost required.
   vii. Review location settings and grant location access only when the app is in use.

d) **Disable Unneeded Network Radios -** Disable radio services like Bluetooth, Wi-Fi, GPS, and NFC when not required. Also, avoid connecting to public Wi-Fi, which is often not secured and can be an attack vector.

e) **Install Security Software -** Security software (mobile antivirus etc.) protects against malware infection and should be installed from verified vendors/sources.

f) **Use Trusted Chargers or PC Cables -** A malicious charger or PC can load malware to the smartphone and may take control of them. Users are advised to use the genuine charger and connect cables only to a trusted PC/Laptop for charging or data transfer. Avoid charging your mobile phones at public charging stations (juice jacking).

g) **Safe Browsing Practices -** Users are advised to follow following safe browsing practices.
   i. Never click on links with promises that are too good to be true.
   ii. Avoid clicking on web links from unknown sources. Stay away from suspicious websites when browsing because it may lead to malicious websites that can affect the smartphone severely.
   iii. Be Careful About Hyperlinks and Ads.

iv. Blocks Pop-up by default and allow them on a need basis carefully. They can be dangerous for your browsing experience because they may contain ads, harmful links, and inappropriate content.

h) **Avoid jailbreaking or rooting your phone**- Users should not jailbreak or root their phone to gain access to some applications or services. It makes the phone highly vulnerable to cyber-attacks as all the security of the phone strips away while jailbreaking the phone.

i) **Backup Data** - Users are advised to back up their phone data regularly manually or using automated services. Mobile devices have the option to back up device data to the cloud automatically.

j) **Delete Data Before Discarding the Device** - Before discarding a device, to ensure data is not misused; it is advised to delete all the data from the mobile device.

k) **Use Bot Removal Tool** - Users who suspect their smartphones to be infected are advised to visit the "Cyber Swachhta Kendra" website https://www.csk.gov.in/security-tools.html and download free bot removal tools. Users can scan and remove bots from their devices using these tools.

(Rahul Modgil)
Chief Information Security Officer

To,

1. OSD to CPFC – for information of CPFC
2. FA&CAO
3. CVO
4. All Addl. CPFCs (Zones/Head Office)
5. Director (PDNASS)
6. CTO
7. All Regional PF Commissioners
8. In-charge of the Regional Offices including RPFC (ASD), Head Office