Subject: **Advisory- Prevention Against Cyber Espionage (Advisory No 19) Apr 18**

1. **Introduction.** A malware campaign named **"RottenSys"** has affected nearly 5 million android devices worldwide. The malware disguise as **"System Wi-FI service"** app that comes pre-installed in brand new devices by popular smartphone manufacturers.

2. **Affected Products.** All affected devices were shipped through Tian Pai, a Hangzhou-based mobile phone distributor. Manufacturers of these devices are listed below:-

a. Huawei
b. Xiaomi OPPO
c. Samsung
e. GIONEE

3. **Technical analysis**

a. App takes all sensitive Android permissions and communicate with C&C to get malicious code.

b. Enables DOWNLOAD_WITHOUT_NOTIFICATION to avoid and user interaction. This enables malware to further download applications and UI automation.

c. App generates advertisements aggressively to generate fraudulent revenues.

d. All infected devices become a part of massive botnet network.

4. **Mitigation Method**

a. In order to check if device is infected ,go to Android system settings App Manager and look for the possible malware package names:-

(1) com.android.yellowcalendarz
(2) com.changmi.launcher
(3) com.android.services.securewifi
(4) com.system.service.zdsgt

b. If any of above is in the list of your installed apps, simply unin tall it.

5. **Recommendations.**

a. Strictly follow all mitigation measures discussed at para 4.
b. **Install and update well reputed antiviruses for Android sMartphones.**
c. Update Mobile OS and applications regularly.

d. Download and install applications only form Google Playstore and avoid third-party sources.

e. Don't download attachments from emails Unless you ate sure about .the sources.