***IN* INFOSEC ADVISORY – 01/ 2023**

MOBILE BASED MALWARE : METHODS AND COUNTERMEASURES

1. India's digital landscape has witnessed tremendous growth, with over 80 crore Indians actively utilising the Internet and cyberspace, making it one of the largest connected nations in the world. Recognising the significance of a secure and trustworthy digital environment of India, GoI and the Armed Forces have formulated various policies, guidelines and advisories for secure use of Internet. The growing cyber threats and attacks have necessitated the need for educating and sensitising the naval fraternity on methods of cyber-attacks perpetrated through various malware.

2. **Aim**. The aim of the advisory is sensitise the environment on the modus operandi of mobile based malware and precautionary measures to be taken.

3. **What is Mobile based Malware**. Mobile malware is malicious software specifically designed to target mobile devices, such as smartphones, smartwatches and tablets, with the goal of gaining access to private data.

4. **Types of Mobile based Malware**. Malware attacking mobile platforms can be categorised based on their functionality. This helps to develop a better understanding of the threats and deploy mitigation in precise and optimised manner.

5. Various types of Mobile based Malware are as follows:-

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

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

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

   (d) **Adware**. Mobile Adware is unwanted software designed to serve advertisements on your device. These are mostly bundled with genuine software. Some Adware also track user behavior.

   (e) **Crypto Currency Mining Malware**. This type of malware uses device resources to perform complex calculations needed to generated crypto currency (cryptojacking).

   (f) **Remote Access Tools**. These tools are used to access a device remotely and take complete control over the device viz., over installed applications, call history, address book, web browsing history, SMS, etc.

(g) **SMS Trojan**. These Trojans use the SMS of a mobile device to send and intercept messages.

6. **Methods of Modern Mobile Malware**. Methods used to deploy malware in target systems are as follows:-

(a) **Fake Calls**. Trojans can masquerade as banking apps and imitate phone conversations with bank employees. Such Trojans take various permissions during installation, such as access to contacts, microphone & camera, geo location, call handling, etc. These Trojans use their own interface to initiate and receive phone calls. Instead of connecting to the actual bank, these Trojans connect to the attackers who, under guise of a bank employee, try to coax payment data or other confidential information out of the victim.

(b) **Fake Applications**. These are applications in a mobile app store or on websites that entice users into downloading them by using legitimate company names or popular references. Once installed on a mobile device, these fake apps can perform various malicious activities. They can persistently push ads, track & report location and other sensitive information or subscribe users to premium services without consent.

(c) **On-Device Fraud**. On-Device Fraud (ODF) is a new technique in which fraudulent activities are initiated on the victim's device. Trojans like Octo, Tea Bot, etc., have been found using ODF. In these cases, the Trojan utilises the device's genuine services. For example, Octo uses Media Projection and Accessibility Service in Android, which gives an attacker remote control over the device, which is then utilised for ODF.

(d) **Bypassing App Store Detection**. It has been observed that malware developers have been successful in bypassing security review protocols designed by Apple and Google for preventing malicious apps from being published. "CryptoRom" app on iOS and the "Color Font" app on Android are recent examples.

(e) **Notification Direct Reply Abuse**. Mobile malware like FluBot, SharkBot, Madusa, etc., have been found abusing the Direct Notification Feature of Android that allows intercepting and direct reply to push notifications. It could be used to sign fraudulent financial transactions, intercept two-factor authentication (2FA) codes, and modify push notifications.

(f) **Domain Generation Algorithm**. Like conventional malware, mobile-based malware is also found to use a Domain Generation Algorithm (DGA), which makes detection difficult.

(g) **Miscellaneous Methods**. Mobile-based malware are also using design practices like accessibility engines, infrastructure and C2 protocols that enable them to update their capabilities.

7. **Countermeasures and Best Practices for Mobile Device Users**.

(a) **Keep OS and Apps updated**. Users should always check and ensure that their mobile devices are running on the latest operating system (Android, iOS, etc.)

(i) Users should enable auto-updating features for the operating system and mobile applications to get the latest security, privacy and flaw fixes.

(ii) User should be aware of the updates cycle followed by the OEM. System updates and security fixes are mostly issued for a duration of two to three years, depending on make and model of the handset.

(b) **Use Strong Authentication**. Users should use strong login passwords/ PINs and use biometric authentication (on supported devices). In addition, users are recommended to use two-factor authentication (2FA) for apps that support them.

(c) **Apply Mobile Application Security Measures**. Users are advised to adhere to the following measures for mobile security applications:-

(i) Disable third-party app stores or any other unknown standalone sources as they can be vectors for spreading malware.

(ii) Avoid installing apps from unknown sources.

(iii) Periodically review mobile apps and delete applications which are not used or not needed.

(iv) Minimise Personally Identifiable Information (PII) data such as address, e-mail, Govt issued ID card numbers, etc. stored in apps.

(v) Review permissions required by each application critically and grant only those permissions which are utmost required.

(vi) Review location settings and grant locations access only when the app is in use.

(vii) Pay attention to the permission sought by the apps while installing and review them periodically.

(viii) Don't hand over your phones to strangers pretending to be not having a phone and need to make an urgent call. In cases where the requirement is considered to be genuine, dial the number yourself and keep the phone in your sight at all times.

(ix) Restart your mobile phone on daily basis or schedule the same in settings.

(x) Factory reset your mobile phone on suspicion of malicious activities.

(d) **Disable Network Radios when not required**. Disable radio services like Bluetooth, Wi-Fi, GPS, and Near Field Communication (NFC) when not required. Also, avoid connecting to public Wi-fi, which is often not secured and is a very common attack vector.

(e) **Install Security Software**. Security software like mobile antivirus protects against malware infection and should be installed from verified vendors/ sources. Additionally, it is advised to install 'mKavach 2.0' application on personal Android Mobile phones. The application is available on Google 'Play Store' as well as 'mseva Appstore' of GoI developed by 'C-DAC, Hyderabad'.

(f) **Use Trusted Chargers or PC Cables**. A malicious charger or PC can load malware to the smartphone and take control of them. Users are advised to use a 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, especially at Railway Stations, Airports, etc.

(g) **Avoid 'Jailbreaking' or 'Rooting' your Phone**. 'Jailbreaking' or 'rooting' refers to the practice of removing software restrictions imposed by the manufacturer. Users should not 'jailbreak' or 'root' their phone to gain access to some applications or services. This practice makes the phone highly vulnerable to cyber-attacks as the manufacturer-imposed security of the phone cease to function while jailbreaking the phone.

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

(j) **Delete Data before Discarding the Device**. Before discarding a device, it is advisable to delete all data from the mobile device or factory reset the device so as to ensure data is not misused.

(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.

(l) **Disable Ad tracking**. The ad identifier "IDFA (Identifier for Advertisers)" on iOS, or "AAID (Android Advertising ID)" on Android is the key that enables most third party tracking on mobile devices. Disabling it will make

it substantially harder for advertisers and data brokers to track and profile a user and will limit the amount of personal information that reaches the advertisers. Procedure to disable the tracker is as follows:-

(i) **Disabling Tracking on Android (Android 12 onward)**. Open "Setting" App and navigate to "Privacy>Ads". Tap "Delete advertising ID", then tap it again on the next page to confirm. This will prevent any app on your phone from accessing it in the future.

(ii) **Disabling Tracking on Android (Prior to Android 12)**. The 'Opt out' functionally mentioned in preceding para is not available prior to Android 12 release. The older version of Android's privacy controls can be used to reset in such conditions to avoid tracking by Apps.

(iii) **Disabling Tracking on iOS**. Apple requires apps to ask permission before they can access your 'IDFA'. When you install a new app, it may ask you for permission to track you. Steps to disable the tracking are as follows:-

(aa) Select "**Ask App Not to Track**" to deny it 'IDFA' access.

(ab) To see which apps you have previously granted access to, go to Settings> Privacy> Tracking.

(ac) Here you can set the "**Allow apps to Request to Track**" switch to the "Off" position (the slider is to the left and the background is gray). This will prevent apps from asking to track in the future. Additionally, you can disable tracking for individual apps that have previously received permission.

(iv) **Disabling Apple's own Tracking**. Apple has its own targeted advertising system, separate from the third-party which is enabled using IDFA. To disable it, navigate to Settings> Privacy> Apple> Advertising. Set the "**Personalised Ads**" switch to the "Off" position to disable Apple's ad targeting.

(m) **Safe Browsing Practices**. Users are advised to follow the following safe browsing practices:-

(i) Never click on links with promises that are too good to be true or seem to convey a sense of urgency.

(ii) Avoid clicking on web links from unknown sources. Stay away from suspicious websites when browsing, as it may lead to malicious websites that can affect the smartphone severely.

(iii) Be careful about hyperlinks and ads. Inspect links thoroughly before clicking.

(iv) Block pop-ups by default and allow them carefully, only on need basis. Pop-ups can be dangerous for your browsing experience as they may contain ads, harmful links, and inappropriate content.