certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2017-0040

Smartphone Security

Original Issue Date: August 30, 2017

Description

Smartphone is a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded apps. Users rarely secure their mobile device, making it a target rich environment for malware. Malicious apps have been found in the app store and unintentional download of malicious software are just a few examples of infection methods. Once such malicious software is downloaded, attackers can force a device to perform certain tasks on a user's device such as such as recording audio and video, sending out data including text messages, contacts, personal images, videos, locations etc., opening webpages, stealing user data, deleting/encrypting files, performing untrusted inputs to applications and various other attacks.

However traditional computer security technical measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers. Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts. Unfortunately, many smartphone users do not recognize these security shortcomings. Many users fail to enable the security software that comes bundled with their phones, and they believe that surfing the internet on their phones without enabling security software is as safe as or safer than surfing on their computers.

Attack Vectors

- Fake applications: These are applications in mobile app store or on websites that trick users into downloading them by using legitimate company names or popular references. Once installed on a mobile device these fake apps can perform a variety of malicious activities. They can persistently push ads, track and report location and other sensitive information, or subscribe users to premium services without consent.
- Data leakage: A phone with no protection allows an attacker to access all the data on it. The phone is usually disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it. Most apps have privacy settings but many users are unaware of these settings. The risk imposed by default settings is that the data may be transmitted to remote locations, not under the control of a user.
- Mobile Phishing - It is much harder to recognize a phishing email when viewing it through a mobile app. It's equally difficult to spot a phishing page. The same is true for SMS text messages that purport to come from trusted and legitimate sources. Attacker can collect user credentials (e.g. passwords, creditcard numbers) using fake apps or (sms,email) messages that seem genuine.
- Ransomware attacks - A ransomware locks all files/data by encrypting them. To regain access to them, one has to pay the "ransom" in the form of a digital currency or a prepaid card. Ransomware spreads through unsolicited email attachments, MMS, infected apps and compromised websites.

Best practices for users

- It is always best to go to official app stores for downloading applications securely. Always check for app details prior to download. Reading every tiny detail of the app policy can aid to weed out the fake or malicious apps. Check what permissions the app requires. If the permissions seem beyond what the app should require, do not install the app.
- Various apps may seek your permission to record audio and video, sending out data including text messages, contacts, personal images videos, locations etc. You should weigh the risks with the benefits that these apps offers. Users should look at granting appropriate permissions to such apps with utmost care.
- Maintain physical control of your device, especially in public or semi-public places.
- Disable interfaces such as Bluetooth, infrared, or WiFi when not in use. Attackers can exploit vulnerabilities in software that use these interfaces by carrying out malicious code in an attractive package.
- Never click on links with promises that are too good to be true.
- Always be in the know of security features installed on the mobile devices.
- Have a decent password and use encryption: Most of the smart-phones enable its users to lock the device with a PIN or combination. It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone. Encryption shields ones data stored on the phone or in the memory card.
- 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 smart-phone severely.
- Avoid jail-breaking or rooting your phone: Think twice before jail-breaking or root your phone to gain access to some applications or services. It makes your phone highly vulnerable to cyber-attacks as all the security of your phone strips away while jail-breaking your phone.
- Update apps as often as possible: With each app that remains outdated, including browsers, one's phone is more vulnerable to infections.

- Update OS: Apply any security updates issued by their carrier or device manufacturer as they become available. Mostly users don't update their OS. Updating phone software requires ample memory and users are often running low on it. Every time a software update is delayed on a mobile phone, the attacker has an opportunity to exploit vulnerabilities in the OS.
- Set Bluetooth to an `Invisible' mode: Leaving your device's Bluetooth visible to all alerts attackers to find your device and make an unwanted connection. So it is always better to select the `invisible' mode and remain invisible to unauthenticated devices.
- Disable interfaces when not in use: Leaving interfaces like Bluetooth, WI-Fi, infrared etc `on', when they are not in use can make it easy for attackers to exploit vulnerabilities of the software used by these interfaces.
- Avoid unknown Wi-Fi networks: Avoid connecting phones to unsecured wireless networks that do not need passwords to access. Many attackers are known to have a penchant in creating phony Wi-Fi hotspots. These wireless networks are specifically designed to carry out a `man-in-the-middle' attack

to gain access to the smartphone.

- Back-up your data: There is nothing worse than losing all your contacts, pictures, and other sensitive data stored in your phone to a cyber attack. So, to lessen the damage caused by an attacker, it's wise to back-up your phone's content or synchronize the information regularly. Most of the devices available in the market have option for automatic backup in cloud.
- Use social media networking applications carefully: Using social media apps may reveal users' personal information to other users, even to the unintended parties on the Internet with malicious intentions. Smart-phone users specially need to be careful while using applications and services on social media that can track their locations.
- Delete data before discarding the device: It's very important to delete all your data from your mobile phone before discarding it, to avoid having your personal information compromised. Users can check with their mobile phone developers for getting useful related information on Factory reset/wiping the device securely.
- If you feel or suspect your smartphone is infected, you may visit Botnet Cleaning and Malware Analysis Centre website (http://www.cyberswachhtakendra.gov.in) for the remedial measures.
- You may also download M-Kavach tool from Botnet Cleaning and Malware Analysis Centre website (http://www.cyberswachhtakendra.gov.in) to address threats related to malware that steal personal data & credentials, misuse Wi-Fi and Bluetooth resources, lost or stolen mobile device, spam SMSs, premium-rate SMS and unwanted / unsolicited incoming calls.

References

https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf
https://usa.kaspersky.com/resource-center/threats/smartphones
https://blog.networks.nokia.com/mobile-networks/2016/07/04/smartphones-new-attack-vector-hackers/
https://heimdalsecurity.com/blog/smartphone-security-guide-keep-your-phone-data-safe/
http://www.cyberswachhtakendra.gov.in
http://www.abc.net.au/news/2016-03-10/cybercriminals-target-millions-of-bank-app-users/7237220
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India