

## Safeguarding Smart Phones against Cyber Attacks

### **1. Description**

Smart phones that are available these days in the market are powerful enough to perform many of the operations of a PC. But, unlike conventional computer security, which has firewalls and antivirus measures regularly updated, smart phone security has failed to keep up with the pace and hence become a catalyst for launching cyber-attacks on the go.

Equipped with a multicore processor, coupled with significantly high memory & storage, these phones can easily be turned into a cyber-weapon to carry out attacks. These devices are vulnerable to various kinds of exploits, bots and remote access tools (RATs), which are often found in third-party app stores. These gadgets can be used to conduct small-scale DoS and SQL based attacks from applications found in the app store.

Mobile devices are highly vulnerable to malware and users rarely secure their device, making it a target rich environment. Malicious apps found in the app store and drive by download are just a few examples of infection methods. Using RATs, **attackers can force a device to perform certain tasks such as recording audio and video, sending text messages, opening webpages, stealing user data, deleting/encrypting files, launching DoS attacks via HTTP floods, performing Web injections and various other attacks.**

### **2. Attack Vectors**

#### **a. Denial of Service attacks**

When an attacker creates either a large number of requests or specifically crafted requests or both at the same time to cause a client's device to stop responding. A DoS variant where attackers employ multiple machines (computers, servers, and mobile devices) to carry out a Denial of Service attack simultaneously, thus increasing its effectiveness is called as "Distributed Denial of Service" attacks. Nowadays a new wave of DoS attacks surfaces known as "DNS amplification attack". This is a two-step sophisticated DoS attack: Firstly, the attacker spoofs the IP address of the DNS resolver and replace it with the victim's IP address, so that all DNS replies will be sent to the victim's servers. Second, the attacker find an Internet domain that is registered with many DNS records. During this attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. The DNS server's replies are usually so big that they need to be split over several packets.

#### **b. Cryptocurrency mining**

A malware involved in the mining for various digital currencies. The miner will run in the background once it detects that the affected device is connected to the Internet. By default, it launches the CPU miner to connect to a dynamic domain, which then redirects to anonymous mining pools.

### c. 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.

This makes mobile devices more susceptible to phishing attacks. The same is true for SMS text messages that purport to come from trusted and legitimate sources.

### d. Ransomware attacks

A ransomware locks all files 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 email attachments, MMS, infected apps and compromised websites.

## Best practices for users

- a. **Have a decent password and use encryption:** Most of the smartphones enable its users to lock the device with a PIN or combination. It is advisable for users to enable encryption, remote wipe abilities and antivirus software on the phone. Encryption shields ones data stored on the phone or in the memory card.
- b. **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.
- c. **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 cyberattacks as all the security of your phone strips away while jail breaking your phone.
- d. **Install new applications with caution:** A little research about the app you wish to download is always a good idea before actually installing it on your phone. It's a good idea to read reviews of each app you plan to download and pay attention to the permissions it asks for. If the permissions sound unreasonable and beyond what the app should be asking for, then the app may be a Trojan horse carrying malicious code.
- e. **Update apps as often as possible:** With each app that remains outdated, including browsers, one's phone is more vulnerable to infections.
- f. **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.
- g. **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.
- h. **Disable interfaces when not in use:** Leaving interfaces like Bluetooth, WiFi, 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.
- i. **Avoid unknown WiFi 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 WiFi hotspots. These wireless networks are specifically designed to carry out a "man-in-the-middle" attack to gain access to the smartphone.

- j. **Backup 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 phones content or synchronize the information regularly. Most of the devices available in the market have option for automatic backup in cloud.
- k. **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. Smartphone users specially need to be careful while using applications and services on social media that can track their locations.
- l. **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.