

With the increasing number of people using smartphones powered by android operating system, there is a challenge, which the users are facing. The number of malware attacks on android smartphones is increasing day in day out. This is creating many problems to users and it is essential that people learn how to protect their phones from such invasions.

According to a report released by Kaspersky, the number of attacks perpetrated on android devices has tripled from the first quarter to the second quarter of 2012. Kaspersky has hinted that in the second quarter of 2012, attacks on android iOS reached close to 15,000 malware. This figure is up from about 5,500 malware, which were recorded in the first quarter of 2012.

This suggests that there is an increasing target of android iOS by malware attackers and this is something that should sound an alarm to the device users. Androids are used by business people who carry out transactions online. This means that if their banking information is compromised; they are likely to lose their money.

In addition, users also store personal and business data on these devices and if intruders have access to such information, they can use it to sabotage their businesses. What this means is that users of these devices should get information on the nature of malicious software they are likely to encounter when using their phones. The more information they get, the more they are likely to keep away from these attacks.

Some of the malicious software like Trojan may come in form of multiple bundled apps, which look attractive to unsuspecting users. As soon as the users click on those apps, their devices are infected. When the infected phones are rebooted, the software launches in the background and begins to broadcast the device's phone number, IDs and other confidential details.

The malicious software uploads that information on a command and control server. The most targeted android users are those with premium accounts. Moreover, those people using these devices for mobile SMS payments are also at risk from the attacks. Recently, a Trojan malware was encountered by mobile phone subscribers in China and this affects functionality of SMS operations.

This could be devastating considering that many people are turning to mobile payment because of its convenience. The Trojan takes control of the SMS functionality of the devices and can send, forward and drop SMS contents on the phones. Worst of it all, even when it is discovered, the malware is difficult to uninstall from the smartphones.

This means that a removal tool has to be released to the apps store so that users can download it and remove the malware. The Trojan is able to generate unauthorized payments and also steal credit or debit card numbers. It is also able to steal money transfer receipt information. This means that it could be difficult to detect payments that are initiated by the malicious software. In essence, there is a new wave of malicious codes, which are targeting iOS smartphone users, and people need to know how they can prevent such attacks.

[telefon dinleme](#)