

Smartphone virus attack soars as malicious programmers are always looking for new targets. While smartphones and tablets replace PCs as the gadgets we use for messaging, Web surfing and even doing business, cybercriminals are starting to target these devices with new forms of Trojans and spyware.

Hackers are following prey onto smartphones and social networking hotspots, according to reports released Tuesday by Symantec, stated in the latest volume of its Internet Security Threat Report. Cyber criminals are also increasing the sophistication and frequency of attacks on business and government networks. Symantec also depicted a "massive" volume of more than 286 new computer threats on the Internet last year, a continued growth in attacks at online social networks and "a notable shift in focus" by hackers to mobile devices.

In recent months, smartphones running on Google-backed Android software were the target of the largest attack ever on the devices, noted a PandaLabs report. PandaLabs said "This assault was launched from malicious applications on Android Market, the official app store for the operating system,"

The purpose of attacks was mostly unclear. But one app used a phone's locating software to transmit the owners' whereabouts without permission. Another was designed to quietly send repeated text messages, while charging hefty fees to the owner's wireless account.

The number of threats is very small compared with the vast array of malware targeting PCs. At this moment, some experts believe it's more important for smartphone users to follow common-sense precautions than to purchase one of the commercial antivirus products now offered for mobile devices. But even though the most popular smartphone operating systems may be less vulnerable than PCs, experts say the growing popularity of mobile gadgets means malicious coders will inevitably target them more often in the future.

It is expected that the number of smartphone users worldwide will exceed the one billion mark

by 2013, with growth driven by ongoing competition between top tier OEMS and challengers such as Google, RIM, Apple and Microsoft, all of which are racing to create the best possible user experience at lower pricing points.

Although Symbian currently leads the market, Android will become the most popular brand in the mobile OS market and is expected to attract more than half a billion users by 2015, according to the latest forecasts from Informa Telecoms & Media. Meanwhile, the number of Android users is expected to grow very rapidly thanks to the strong support by almost all major players in the mobile industry value chain – with the exception of Nokia. In fact, this platform is currently supported by some 200+ regional mobile operators and 20 top tier vendors.

Today, about 100 Android smartphone models and variants have been launched worldwide, targeting different segments of the smartphone market. Nine out of ten smartphone owners use the device to browse the Internet, but only 6% have antivirus installed, finds survey. Therefore, many are often unaware of the malware threat on these devices and do not feel the need to protect their phones.

A survey commissioned by Slovakia-based security company ESET has found that a high number of smartphone users are at risk of losing data because of a virus attack. The research revealed that 31% of consumers do not even know their smartphone is at risk of viruses, while 14% assume security was built into the phone when they bought it.

Smartphone virus attacks are very common these days. The number of virus attacks is only going to increase if organizations fail to pay attention on the vulnerabilities of their mobile security. Organizations need to enforce robust information security initiatives, including having a proficiently skilled IT security workforce, in order to prevent cyber attacks and minimize security breaches. Information security professionals can increase their IT security knowledge and skills by embarking on advanced and highly technical training programs.

[telefon dinleme](#)