

# Act smart to save your smartphone from the bad guys

JUDHI PRASETYO

**M**obile phones and other wireless devices are the new weakest link in securing information outside corporate networks.

We all know that “bad” guys take notice of new technology and create attacks based on the latest trends. So, how are enterprises keeping up? With mobile usage of Facebook and Twitter rising, users can affect enterprise networks easily without knowing. What are some best practices and concerns to avoid horrible issues? What should wireless gurus know about unforeseen security issues created through wireless devices?

While malicious activities on handheld devices such as smartphones have been relatively low, there are several indicators to suggest that things are about to change. Enterprises will need to start thinking seriously about a mobile threat prevention strategy to ensure that their networks are not vulnerable to the new threats that will abound with the increasing mobile activities of their users.

The growing prevalence of 3G networks is enabling broader bandwidth for mobile devices, which means more bad content is getting in with the good. 3G also enables network operators to offer a wider range of more advanced mobile services, such as real-time access to high-quality audio/video transmission. For example, with its application portal, Apple, which has a small percentage of the handset market, has already changed the way many people interact with their smartphones, while Microsoft and Nokia are also talking up their own similar portals. The level of personalisation and customisation possible with these portals will mean new uses, both good and bad, will be found. This presents a big concern for corporate



Fortinet believes the increased usability of smartphones and other wireless devices and the new business models they enable will become the biggest threat to corporate security in the near future.

The mobile market presents a unique position in terms of malware as compared to the traditional PC market. The platforms available for attack on PC platforms are limited – Windows, MacIntosh and Linux – while the number of mobile platforms continues to grow: Google Android, Apple mobile OS, SymbianOS, Windows Mobile and Palm. For example, we are just seeing the tip of the iceberg with Google’s Android OS vulnerability discovered late last year. And just last month, discovery of the new SymbOS/Yxes.A!worm mobile worm gives strong indication that we may be on the edge of a mobile botnet. This sophisticated SMS-propagation strategy, which hosts the worm on malicious servers, allows cybercriminals to effectively mutate the worm by adding or removing functionality.

network managers as users are no longer bound by factory-installed applications. With this greater usability, consumers are now adopting smartphones in greater numbers for business and for personal use. Research group iSuppli predicted in its March report that the number of smartphone shipments is expected to grow to as high as 192.3 million units this year, up 11.1 per cent from 2008.

Where consumers go, money goes, and crime will soon to follow. This adds up to increased opportunities for virus infections and attacks that will require a focused approach to secure the millions of handheld devices in operation today, especially for enterprises. Smartphones pose an even greater security risk to corporations as they have become the mobile office for their ability to access corporate networks in real time, much in the way that laptops have been able to do. This presents cybercriminals with the opportunity to use smartphones as the launch pad for accessing corporate data.

A managed client capable of detecting software installations and monitoring file access in addition to encrypting data and reporting status to a central server is the answer for network managers grappling with an active mobile workforce. Network managers will want to look for solutions that provide multi-layered protection for blended threats and that protects across all device interfaces. The ideal mobile client solution would be part of an integrated, end-to-end network security platform that offers accelerated hardware and impinges minimum performance impact on user device and services. In addition, the network security platform should offer configuration management and control with reporting, and flexibly-defined profiles and policies for network segmentation capabilities.

■ *The author is the Regional Channel Manager Middle East at Fortinet, a provider of network security appliances and in the unified threat management market worldwide*