

'As security companies we must provide multiple layers of defence to protect our users properly.'

Robert Sandilands, Authentium

WHAT IS ANTI-VIRUS SOFTWARE?

As we near the end of 2007 you will find that anti-virus is no longer software that 'just' detects viruses. As a result of the changes in computers and their purpose, anti-virus programs have evolved into complex pieces of software that have multiple functions and protect users through a variety of techniques.

In the past, most pieces of malware were badly written and full of bugs and their effects could easily be identified by the average user. But malware writers are increasingly becoming very professional, with viruses being written on demand for specific purposes – such as stealing your money, stealing your identity or using your machine as a spam-sending zombie.

Many of these pieces of custom-written malware seem to have gone through some form of quality control process and seem to be well managed. The malware also uses a variety of different techniques and components. The components are often self-updating and protect themselves from being detected and/or removed.

One of the basic principles of computer security is layered defence. One should never depend on a single layer of defence, because once that layer is breached it leaves you defenceless. The average modern piece of malware will disable security software as one of its first actions, and once the computer's security has been bypassed you don't get any second chances.

As security companies we must provide multiple layers of defence to protect our users properly. The different layers of defence can include a number of technologies: known-virus scanners, heuristics, host intrusion detection, behavioural blocking or detection, policies (both machine and human-based), reputation-based systems and firewalls. None of these technologies can provide complete protection on its own, but used together they form a good multi-layered package to maximize the user's security.

Known-virus scanners use a variety of techniques to identify known risks. However, malware authors can use several methods to obscure viruses from scanners, with varying levels of success. Heuristic detection uses a combination of the techniques used by the known-virus scanners with some other tricks to determine the likelihood that a specific executable is a threat.

This is where the additional layers of defence prove their worth. The extra levels of protection can mean the difference between making life easy for the criminals and having a secure machine.

Unfortunately, some of these other techniques can affect the user's privacy. The products can report data about the user's habits and the actions of the security software to a central database for use in isolating threats or providing statistics on the size of the threat. Some vendors go to significant lengths to protect the user's privacy, but unfortunately this cannot be generalized.

Other technologies are invasive in a different way. They need to be able to monitor and control the actions taken by the operating system and, effectively, the user. The security software needs to become the watcher that watches the watcher. This is very complex technology that takes security to a new level, as the security software needs to understand the intent of the operating system or user, as well as what he or she is doing. These technologies need very deep access to what your computer is doing and how it is working – indeed this has become one of the sources of debate around *Microsoft*'s *Patchguard* kernel protection technology.

The anti-virus industry needs to and will continue innovating to keep users as safe as technology can make them. Sometimes the environment in which the anti-virus industry has to operate makes this task more complex than it perhaps needs to be. Despite that, the competition that exists in the anti-virus industry will ensure that customers receive innovative products that provide them with the level of security they demand.

Editor: Helen Martin
Technical Consultant: John Hawes
Technical Editor: Morton Swimmer
Consulting Editors:
Nick FitzGerald, *Independent consultant, NZ*
Ian Whalley, *IBM Research, USA*
Richard Ford, *Florida Institute of Technology, USA*
Edward Wilding, *Data Genetics, UK*