



Anti Virus (AV) technology doesn't work

It fails to prevent computers from getting infected with viruses, and this failure contributes to many other security woes that plague the world's computers.

Because viruses spread, hackers find it easier to compromise computers, identity theft and computer fraud are easier to perpetrate. Virus infected computers become a resource for hackers to exploit. Some hackers assemble and control networks of thousands of such computers, and use them to distribute huge volumes of spam, mount sophisticated phishing attacks, and launch targeted "denial of service" attacks on companies.

The level of virus infection is high. It's not an epidemic, it's a pandemic. How bad is it? That depends on how you look at it.

For the home computer user and small-business user, infection is chronic. In June, 2006, Microsoft revealed the results of a 15-month test of its Malicious Software Removal Tool on home PCs and small-business PCs. The utility had been used to scan and clean 5.7 million PCs, and it found backdoor Trojans, or programs that let hackers gain entry, on about 62% of them, and during the 15-month period, 20% of PCs that were cleaned were reinfected.

Faulty 'Burglar Alarms'

So why is it that AV technology does such an inept job? Consider the following information, published last year by AusCERT, Australia's Computer Emergency Response Team.

The most popular AV products fail to prevent 80% of new viruses.

AusCERT declined to name the AV companies publicly, but in case you didn't know, the leading AV vendors are Symantec (Norton), McAfee, and Trend Micro, in that order.

Mind you, it isn't necessarily the case that these products are technically inferior to other AV products, it's just that most virus writers test their viruses against the popular AV products before unleashing them on the world.

Because of this, AV technology is doomed to be ineffective, and it is never going to be effective. The AV vendors have built "burglar alarms" that alert you only if a known burglar tries to enter your house. Any burglar that they don't recognise gets in unopposed. The practical solution is to have a "burglar alarm" that sounds when anyone you don't know tries to enter the house, deceptively simple, isn't it? But security products that work in this way have only recently been introduced.

The first company to offer such a product was SecureWave, in 2001. Since then three other companies, AppSense, Bit9, and Savant Protection have introduced products that work in this way. Instead of focusing on identifying malware, these products manage a full record, a so-called white list, of the valid programs, and prevent other programs from running, or, if necessary, run unrecognised programs in quarantine until their nature becomes clear.

Not Solved Yet

At the moment these products are focused only on the larger company market. As the persistent failure of AV products becomes increasingly visible and as the popularity of these newer products grows, they will become available to the home user. Until then, the computer virus pandemic, and all the evils it engenders, is likely to continue.

www.encryption.co.uk

01905 754440