

Eighty percent of new malware defeats antivirus

By [Munir Kotadia](#), ZDNet Australia

19 July 2006 03:05 PM



The most popular antivirus applications on the market are rendered useless by around 80 percent of new malware, according to AusCERT.

At a security breakfast hosted by e-mail security firm Messagelabs in Sydney on Wednesday, the general manager of the Australian Computer Emergency Response Team (AusCERT), Graham Ingram, told the audience that popular desktop antivirus applications "don't work".

"At the point we see it as a CERT, which is very early on -- the most popular brands of antivirus on the market ... have an 80 percent miss rate. That is not a detection rate that is a miss rate.

"So if you are running these pieces of software, eight out of 10 pieces of malicious code are going to get in," said Ingram.

Ingram, who refused to name any specific companies, was quick to point that this was due to cybercriminals designing their Trojans and viruses to bypass detection rather than a defective product.

"I am not suggesting that there is a difference in the quality of the antivirus products themselves. What is happening is that the bad guys, the criminals, are testing their malicious code against the antivirus products to make sure they are undetectable. This is not a representation of the software," said Ingram.

Although less popular antivirus applications are more likely to pick up new malware, Ingram said that the average level of new malware that is undetected is 60 percent, which is "worrying".

"What do most people have as protection for their client machines? I would suggest it is antivirus. You are lucky if you have antispyware. So they are attacking a machine that is protected by a piece of software that is [not working](#).

"This is the dilemma that is building up here and the success rate is becoming quite worrying," added Ingram.