

advertisement · explore within this space

STRETCH YOUR IT DOLLAR EVEN FURTHER
THIS TAX-TIME WITH **HP PRINT LOYALTY**

To print: Select **File** and then **Print** from your browser's menu

This story was printed from [ZDNet Australia](#).

McAfee CEO: Adware is killing AV blacklisting

By [Liam Tung, ZDNet.com.au](#)

June 13, 2008

URL: <http://www.zdnet.com.au/news/security/soa/McAfee-CEO-Adware-is-killing-AV-blacklisting/0,130061744,339289802,00.htm>

Traditional security products — which employ signature-based blacklisting technology — are no longer effective because of a massive increase in malware, according to the CEO of McAfee, Dave De Walt.

Blacklisting — where vendors compile lists of known malware — has become technically unfeasible, said De Walt.

"When you're doubling the amount of malware you're getting on a daily basis, eventually a blacklisting model ultimately could run out of architectural scalability," he said at a press briefing today.

In 2007, McAfee received 370 new malware samples per day, and according to De Walt, that figure is likely to reach 750 per day by end of this year. "The current trend six months into [2008] is we're seeing a doubling of the malware we receive into our labs," he said.



"We're processing gigabytes of malware daily," says Alex Eckelberry, Sunbelt Software.
Source: Sunbelt Software

The gloomy predictions are consistent with other security vendors. Symantec this year said that [65 per cent of the 54,609 Windows-based applications](#) that have been released to the public in the past six months were malicious.

Chia Wing Fei, a security response team manager at F-Secure, told [ZDNet.com.au](#) that in 2007, the company detected more than 500,000 pieces of malware. He expects that figure to double this year — for the second year running.

Late last year, AV testing company, AV-Test produced statistics showing the staggering growth of malware in the past year.

"This is a good representation of the staggering load of malware that anti-malware folks are under," said Alex Eckelberry, a security researcher for security vendor, Sunbelt Software [in response to the statistics](#). "Like most companies, we're processing gigabytes of malware daily."

McAfee's De Walt said he was shocked by the pace of growth.

"This was a shocker to me to see at McAfee just what we face in the world. In 2007, 40 per cent of all malware was written that year," he said.

However, De Walt blames online marketing companies for much of the escalation.

"A lot of it's coming from the growing adware market, which is a legitimate market... Literally billions of dollars are being put into figuring out ways to market more intelligently to you ... in a more personalised way. That's driven malware development.

"Marketing companies often contract companies to figure out ingenious ways to put a brand on your device, and that same ingenious way to put a brand on your device is what potentially the bad guys and

gals can do to exploit your computer — either through data theft, data loss, identity theft or some sort of phishing attack," he said.

As blacklisting becomes increasingly difficult, De Walt said whitelisting technologies hold promise.

"Whitelisting looks like it has an architectural promise that could be very strong," he said.

Whitelisting was a dominant topic at this year's AusCERT conference. Cisco's chief security officer expressed frustration at blacklisting, and said he would like to see more whitelisting. "Antivirus should be an integral part of how you clean content, and keep it safe, however as a first line of defence, I just don't see it anymore," [Stewart told ZDNet.com.au](#).

AusCERT general manager Graham Ingram backed Stewart up. "I think [whitelists] are a natural progression... I think the realisation [is] that blacklisting only had a limited life and we're getting towards the end of that," said Ingram.

However, De Walt has reservations about its adoption due to cultural factors.

"The cultural adoption of it has been the challenge. Because what is whitelisting? You can only use seven products on your machine, you're not allowed to use another product on your machine. I lock down your environment, according to a whitelist and I prevent software moving onto that computer, unless I grant that access to that application," he said.

"The cultural aspects are, I'd really like to use iTunes, or the latest peer to peer music sharing product. That prevents that. It also keeps it safe, but at the same time, it's culturally inhibiting in the way people like to work with their machines."

Copyright © 2008 CNET Networks, Inc. All Rights Reserved.

ZDNET is a registered service mark of CNET Networks, Inc. ZDNET Logo is a service mark of CNET NETWORKS, Inc.