



TECHNOLOGY INSIGHTS

2008 Internet Security Suites Tested Are they getting the Message?

Part 4 - Final Thoughts

Surprises

You would expect long-established security suites to have a solid grip on handling malware by now, so the poor results posted by Trend Micro and CA in AV-Comparative tests surprised me. A search using the product names and 'av-comparatives' will turn up single product tests that provide more details.

AVG free is one of the most popular products out there, so the poor performance of the commercial version was another surprise, most of all in the pro-active tests run by AV-Comparatives. AVG users would do well to add a second product that offers strong heuristic detection, a HIPS program like Threatfire for example.

Norton and McAfee gave me the biggest surprise with their fresh productions. Gone are the days of lumbering mafia heavies beating up your PC. My first thought was: if it's that easy to do, why didn't they do it long ago instead of dishing out stale products year after year like some state-owned factory behind the old iron curtain. I guess the catalyst was serious competition from vendors offering smarter choices.

Compromise versus Purity

If Norton's transformation is remarkable, some of the old bugbears still dog the new production: the need for reboots after major updates, the heavy-handed messages and more.

McAfee's performance improvement is astonishing and its behaviour is much improved as well – the adware of old is gone, for one thing. It's still more intrusive than the best Internet Security suites, but it's a vast improvement on earlier versions.

That MTP's security pieces aren't in the top rank won't make much difference in real-world use, I suspect. Since the performance hit is so slight, users can easily add a HIPS program to enhance their protection without adding significant overhead.

Of course, products that try to do everything for everybody are compromised by default. Greater rewards await those who're prepared to put in a little more work and select the best components. Even the internet suites in Part 2 vary in their success at forging a few components into a well-working whole. Most of their spam filters range from average to ordinary. If spam is a big issue, specialist applications like Cloudmark might be a better choice.

Theatre

I made some blunt comments about the current testing standards, such as they are. Much of the current testing is a well-rehearsed show that only catches out the actors who didn't learn all their lines. During the final edit of this article, I came across an announcement that the major security

These are our own opinions.

We have no commercial arrangements with vendors.

For more reviews, please contact TECHNOLEDGE.

T +61 2 9909 0246
E info@technoledge.com.au
W www.technoledge.com.au

vendors had met in Bilbao, Spain and agreed to form a new alliance that sets new standards for testing — **SECURITY SOFTWARE INDUSTRY TAKES FIRST STEPS TOWARDS FORMING ANTI-MALWARE TESTING STANDARDS ORGANIZATION.**

Subtitle: **Parties converge to address objectivity, quality and relevance of current anti-malware testing methodologies**

http://www.amtso.org/index.php?view=article&catid=2%3Apressreleases&id=5%3Aformationpressrelease&option=com_content&Itemid=2

It looks like a step in the right direction, but how soon will they take that step and will the news standards be less of a farce than the old ones? Will the results be more open to scrutiny by ordinary users? We can only hope so.

Fear, Doubt and Uncertainty

Meanwhile, the hype of the vendors would have us believe that we're under constant threat from meteor showers of malware. The results of the test labs clearly show that none of the products provide 100% protection. A recent F-secure press release puts it in perspective (not intentionally, I suspect):

'Despite the importance of behaviour-based protection, a core capability of any antivirus solution is the ability to detect malware that is known and can be identified with traditional signature based virus scanning. A test done by AV-Test.org included over 600,000 malware samples. F-Secure achieved a very high detection rate, and was able to detect 978 samples more than Symantec, 42,226 samples that Trend Micro did not detect, and 64,653 samples more than McAfee. F-Secure also detected 105,391 samples that Microsoft's solution missed.'

Suddenly, that few per cent difference takes on distinct shape. What F-Secure didn't mention was that its product still missed a bunch of malware. That's where the theatre comes in: all these vendors claim to keep us safe, yet none can keep out all of the malware – even that which 'is known and can be identified with traditional signature-based virus scanning.'

The promised security is an illusion created to make us feel better for a time. The question is: if these suites don't offer full protection, how come all the PCs connected to the internet aren't infected or part of a botnet by now? So, are we really exposed to this staggering number of vile creatures? Of course not. There are knowledgeable people who don't use any 'anti' software at all and claim their PCs don't get infected.

I'm inclined to believe them, and here's why: I've run half a dozen different AVs on my PCs over the years, among them poor performers like Trend Micro and AVG. I've never had a single infection, but I do observe a few common sense rules for email and surfing the web - http://www.technoedge.com.au/pdfs/driver_training1.pdf

The threats we face are changing rapidly, from random hits to highly targeted shots, from viruses to phishing and other scams. It pays to follow the rules of common sense, regardless of the protection you have in place. And the more common sense you use, the less you rely on your security software to do the heavy lifting.

* * *