

The Limits of Scanning

Opinion: A large test shows that the flood of malware is outstripping the capacity of most detection products to keep up.

By Larry Seltzer

Has the malware problem gotten out of control? An aggressive test of anti-virus products indicates that it has, at least by some measures. It's a tough call.

I worry less and less personally about malware, even though I'm barraged by it day and night. I've got a gateway security device that scans for it with a Kaspersky scanner and my mail server runs Sunbelt Software's Ninja, which uses both Authentium and Bitdefender to scan everything coming through, *and* I have desktop anti-virus on almost all my systems. I've got my belt and suspenders and my pants are nailed to my gut.

And it's a good thing I've got all this protection, because tests by independent test group AV-Test paint a dark picture of the detection capabilities of most products.

For many years there has been a standard of sorts for testing anti-virus products called the "WildList." The problem with the WildList is that it's relatively small and contains only certain types of malware, and everyone knows its contents. As Andreas Marx of AV-Test puts it, "the WildList is not reflecting today's threats, but more or less 'historical' threats only (e.g.

which malware was widespread two months ago?)." So it's not surprising that (according to AV-Test) most scanners can detect 100 percent of it. What you should worry about is the huge number of other threats out there.

AV-Test ran a huge test of backdoors (59,053), bots (70,658) and trojan horses (159,971) for a total of 289,682 malware samples. They ran them through 33 products. We have separate numbers on the bots, backdoors and trojans, but check out the table, below, for the ranked results of overall detection percentage.

How do the numbers look? If you ask me, not good. Five vendors scored over 99 percent, which has to be considered excellent in so large a test sample. Another six scored over 95 percent. Another seven were over 90 percent, and this is approximately the median, which was 90.42 percent. Half the products did worse than this; 10 were under 75 percent and four were under 50 percent. That's pretty bad.

Several of the best products, like my own mail security product, use multiple engines. The No. 1 product, Webwasher by Secure

RANKED RESULTS

#1	Webwasher	99.97%
#2	AntiVir	99.95%
#3	AVK 2007	99.95%
#4	AVK 2006	99.89%
#5	Symantec	99.04%
#6	Kaspersky	98.86%
#7	F-Secure	98.24%
#8	BitDefender	96.51%
#9	Norman	96.34%
#10	Nod32	95.80%
#11	Avast!	95.17%
#12	AVG	94.78%
#13	Fortinet	94.65%
#14	McAfee	93.99%
#15	Rising	91.18%
#16	Panda	90.45%
#17	Dr Web	90.38%
#18	Trend Micro	90.03%
#19	Ikarus	84.77%
#20	VBA32	81.28%
#21	F-Prot	77.88%
#22	Command	77.11%
#23	Microsoft	76.18%
#24	Ewido	74.67%
#25	Sophos	65.55%
#26	eSafe	59.34%
#27	UNA	58.76%
#28	QuickHeal	55.72%
#29	ClamAV	48.71%
#30	eTrust-VET	48.37%
#31	eTrust-INO	41.92%
#32	VirusBuster	40.94%
Median		90.42%

Computing, for example, detected 99.97 percent or all but 87 out of the 289,682 samples. It uses the AntiVir engine (the No. 2 product) in combination with an engine Secure Computing developed on its own. Not all products that use multiple engines score better as a result, as they may configure those engines less aggressively.

Some of the best products surprised me. I didn't expect Symantec to do so well, but hats off to them. People like to complain about them, mostly for reasons unrelated to detection percentage, but this test does seem to show that they have taken detection of non-viral malware very seriously. The other high scorers, AntiVir in particular, don't get a lot of attention in the press, and perhaps we have not done them justice.

Then down in the Hall of Shame section we have many products that can't seem to keep up with the flood of malware. I'll start this list with Microsoft which, at 76.18

percent is seriously third-rate. I expected better from Sophos, although that's based on reputation, not personal experience. The eTrust engines and ClamAV are just where I expected them. Of course, even if they didn't dispute the tests in some way, authors of these products might claim that users are highly unlikely to encounter most of the threats in it.

What does this test show? Is it more important that it's possible for products, especially if they use multiple engines, to detect a very high percentage of attacks? Or that the majority of products let through a very high number of attacks? I have to focus on the latter point. It makes me want to consider, once again, alternative approaches to malware.

Most, if not all of these products, detect many classes of malware generically by common characteristics. I asked Andreas Marx and he confirmed that they didn't break out for this test which detec-

tions were based on specific signatures and which were generic, which is a difficult distinction for an outsider to draw in any case.

But I have to think that the percentage of such detections is increasing over time, especially in products like Symantec's. They can't actually have anywhere near 290,000 signatures.

And then there are many companies trying to come at the problem from the other direction, whitelisting programs that the user should be allowed to run and disallowing everything else. This is an old idea and has proven difficult to manage in the past, and it misses malicious code run through most vulnerabilities like buffer overflows. I hear from just about all of these "alternative" approach vendors and I wonder if their time will ever come, but their mission is becoming more important.

Security Center Editor Larry Seltzer has worked in and written about the computer industry since 1983.

Reprinted from eWEEK, October 2, 2006 with permission from Ziff Davis Media Inc.
©2006 Ziff Davis Publishing Holdings Inc. All rights reserved.

SECURE®
COMPUTING