

## Anti-Virus Testing and Consumer Reports

Friday, 15 September 2006

Consumer Reports recently came under heavy fire from some in the anti-virus industry for creating some 5,500 new virus variants to see how well a dozen leading products fared in detecting the new nasties. More than 100 security experts and executives from companies like Microsoft and HP as well as anti-virus vendors F-Secure, Kaspersky, McAfee, Sophos, Symantec and Trend Micro signed their names to a declaration denouncing Consumer Reports' methods, stating that it is "not necessary and ... not useful to write computer viruses to learn how to protect against them."

Some of the signatories noted -- via various media reports about the scandal -- that with so many viruses already in circulation today (estimates vary from 100,000 to 180,000) it was hardly necessary for Consumer Reports to gin up new ones that could, in theory, be leaked into the wild.

Today, however, I read a rather thoughtful article written by Juergen Schmidt, an editor with the German technology magazine Heise Security. Schmidt picks apart what he sees as the source of the industry's angst on this. He argues that testing anti-virus products against known viruses is a non-starter because the real battle against malicious worms and viruses these days is against previously unknown threats, of which he says about 250 emerge each day.

From the article: "The commandment 'Thou shalt not create new viruses' is a sensible self-imposed commitment by the manufacturers of anti-virus software, which prevents them from creating an atmosphere of threat to promote their products. In contrast, meaningful comparative testing of anti-virus software requires that testers work with self-generated virus variants. Anyone condemning such tests in general is certainly not doing so in the interests of the user."

Schmidt says that in light of the poor job most anti-virus programs do at spotting new threats (without the benefit of code snippets), it is clearly necessary to test anti-virus software using previously unseen malware.

"Known viruses no longer represent any great danger for users with anti-virus software -- pretty much every product will recognize them reliably. The real danger lies with the estimated 250 new malware programs that are released every day. And recognizing these as a threat is where many anti-virus products still fail miserably."

As I have noted here before, many malware authors are increasingly outpacing the security vendors by automatically updating the genetic makeup of their creations before anti-virus companies have time to ship updates. As a result, we have an industry whose business is predicated on 10 percent to 20 percent of its customers being successfully attacked before it can even begin to respond, according to some estimates.

If you'd care to see a slick, Web-based method some criminals use to evade fresh anti-virus signatures, check out this story I wrote from a few months back about a Russian hacking ring.

But don't take my word for it: Go ahead and submit any new nasty you receive in your e-mail inbox to VirusTotal.com, a free online service that scans files against more than two dozen of the top anti-virus applications. If the nasty is new enough -- i.e., released in the last four to eight hours -- my experience has been that maybe a quarter of those anti-virus products will flag it as malicious or suspicious. For a sobering look at the rate of detection failures, check out VirusTotal's graph here. In the past seven days, only 261 of the 24,190 infected files submitted to VirusTotal for scanning -- slightly more than 1 percent -- were detected as malicious by all of the anti-virus vendors.

In a blog post two weeks ago I included the results of a VirusTotal scan of a worm that was exploiting a freshly patched flaw in Microsoft Windows. More than 12 hours after the thing had surfaced, roughly half of the anti-virus products failed to detect the sample as malicious.

Yes, the anti-virus industry has in large part gotten better with their "heuristic" detection methods that can spot brand new viruses by linking them to previously identified variants. But this technology has a long, long way to go, in my opinion. Anti-virus testing is hard, and is easy to mess up, and maybe virus-writing for the sake of testing anti-virus products isn't the best way to determine the most agile products (I certainly don't agree with some of Consumer Reports' rankings). But it seems to me that we need a better way to advance the debate about improving their performance.

The most innovative idea I've seen so far came in a presentation from Paul Vixie and David Dagon at the DefCon hacker conference in Las Vegas this year. Vixie and Dagon proposed creating a massive malware repository to which all of the anti-virus vendors would automatically submit new samples. It remains to be seen whether the industry considers this a worthwhile endeavor -- and if so, whether it can set aside its notions of competitive advantage to invest any energy or resources in the idea.

Source: [http://blog.washingtonpost.com/securityfix/2006/08/antivirus\\_testing\\_and\\_consumer\\_1.html](http://blog.washingtonpost.com/securityfix/2006/08/antivirus_testing_and_consumer_1.html)