Cybersoft.com

CyberSoft White Papers

Open Letter

To whom it may concern,

CNET's September 21, 2000, review of antivirus products betrayed their readers' trust. Moreover, it did antivirus product users a major disservice. Although this review was presented as being fair and professional, the evidence demonstrates that it was neither.

Consider the following facts.

Quote: "Viruses"

First, it should be noted that the review leveled charges about missing "viruses" against all four products in the test. Note these examples:

Aladdin eSafe Desktop 2.2

- Virus defense leaks like a sieve.
- Missed half of our test viruses.
- Let our test PC get more infections than there are in a hospital ward.

McAfee VirusScan 5.1

- Missed more viruses in our tests than [Norton] AntiVirus.
- It let more file-carried and email-borne viruses through in our tests.
- It missed three of our nine test viruses.

Norton AntiVirus 2001

- Doesn't protect against Internet-borne viruses as well as McAfee.

- One test virus got through.
- AntiVirus blithely let [a downloaded, virus-infected file] through.

Trend PC-cillin 2001

- Three in nine viruses got through.
- Fails to finger every incoming virus.
- It lets too many viruses through to be considered safe.

Unfortunately, neither the methodology nor result reports indicate exactly what "viruses" were used or which "viruses" were not detected by each product. However, what the methodology does indicate is that some of the "viruses" used in the test were not actually viruses. The section on "How We Tested" states:

CNET Labs used Rosenthal Utilities, a program that simulates viruses, to test for virus detection in main memory, in the file sector of floppy disks in A: drive, on the hard drive, and in the boot sector of floppy disks in A: drive.

In addition to these simulated viruses, CNET did use some real viruses, but the number, ratio and identity of the real and simulated viruses are not disclosed. Only a couple were identified by name. Credible antivirus tests include detailed information on the viruses used and which viruses were missed by each product.

Yet more important than numbers and names is the fact that simulated viruses are not real viruses and using them will skew testing beyond the point of credibility.

To demonstrate this claim, please consider the following information.

Today's antivirus products use a variety of sophisticated methods to detect viruses. Such methods include execution analysis, code and data mapping, virtual machine emulation, cryptographic analysis of file sections, etc.

Such advanced antivirus systems make virus simulation for testing virtually impossible. This is because there is no way to know what sections of viral code and/or data are targeted by any given product. That being the case, all of the virus code and data must be in the file and in the correct order for the product to detect it as that virus. If a simulator did create a file with everything possibly needed in place, it would have to create the virus exactly. It would no longer be a simulator and the virus would be real, not simulated. Therefore a virus cannot be reliably simulated.

So simulated viruses cannot reliably take the place of real viruses. This in turn means they are not a measure of an antivirus product's worth. Think about it. If a product does not report a simulated virus as being infected, it's right. And if a program does report a simulated virus as being infected, it's wrong. Thus, using simulated viruses in a product review inverts the test results. It grossly misrepresents the truth of the matter because:

* It rewards the product that incorrectly reports a non-virus as infected. * It penalizes a product that correctly recognizes the non-virus as not infected.

Competent, credible antivirus product reviewers today recognize the need to reflect the real world in their testing. To do so, they focus detection testing on the real-world threat, using real viruses. They focus on viruses reported by the WildList Organization International. True, some may also include other viruses in testing, but they still use real viruses, not simulated ones.

In addition, the documentation provided with Rosenthal Engineering's Virus Simulator clearly states, "These test virus simulations are not intended to replace the comprehensive collection of real virus samples."

Finally, CNET's own answer to the question "How can I test my antivirus software?" Includes the statement, "Most people in the antivirus community consider a "virus simulator" unnecessary and unsuitable for this task." (This is found on CNET's help.com site at http://www.help.com/cat/2/285/287/tip/3920.html?tag=st.hp.ht.txt.tip.)

Furthermore, the methodology does not state exactly what viruses were simulated. Did the simulated viruses represent viruses that would be an actual threat to the reader?

In light of these facts, it becomes evident that a highly questionable review has been published and CNET's credibility has suffered. Yet their credibility has suffered, not just because they used simulated viruses, but also because the reviewer refers to "test viruses" throughout most of the article. As seen in the quotations above, the review continually refers to the "viruses" that were used, whereas the methodology states that CNET Labs used "a program that simulates viruses."

What happens if a reader doesn't read the "How We Tested" page? What will they assume? They would assume that the viruses are real, wouldn't they? Moreover, they'll probably suppose that these "viruses" are a real threat to them.

But beyond that, what happens when the review actually tells them that the testing represents real-world performance, will they believe it? Why wouldn't they?

Consider as an example the case of Aladdin's eSafe Desktop 2.2. CNET reported the following in their review of eSafe under the subhead Horrible Virus Handling.

eSafe's real-world performance stinks. It failed to sniff out half of our test viruses -- the worst score of any virus hunter we examined.

How exactly does the CNET reviewer define real-world performance? The context here implies that it's based on "test viruses" being missed.

The review says they used "nine real-world viruses on each app, from KakWorm to this year's latest global threat, the I Love You virus." Where then do the simulated viruses fit in? Were simulated versions of "real world" viruses used? What were the other seven "real-world" viruses?

This uncertainty leads u more questions. Exactly what "viruses" made eSafe "stink" so much? Were they actually viruses, or were they simulated?

Let's illustrate the extent of this problem by indulging in a conjectural scenario.

Suppose the "viruses" that eSafe missed were all simulated, and therefore not real viruses. If that were the case, then eSafe was correct in not reporting them, wasn't it? Further, if all the other products mistakenly reported simulated viruses as being real viruses, they would be wrong, wouldn't they? Where does this lead us?

Well, if our conjectural suppositions were true then that would mean CNET's reviewer had slurred a product and declared it the worst, because it was the most accurate one tested. This shows why testing with simulated viruses is, at best, misleading.

In light of the above facts, one thing should be quite obvious. Testing antivirus products with simulated viruses is a gross misrepresentation of reality. So, in doing such testing, and thereby publishing a misleading review, CNET has violated the trust of their readers. In addition, CNET's review has done antivirus users a major disservice.

What does this say about CNET?

If on the one hand, the reviewers mistakenly assumed that testing with simulated viruses was OK, then they are evidently not very well informed. In that case, are they actually qualified to do valid testing of antivirus products?

If, on the other hand, they were informed and did know what they were doing, then misrepresenting simulated viruses as "viruses" throughout the review was a deception and products were knowingly misrepresented.

It is quite doubtful that the reviewer had malicious intent. Still, whichever case is true, CNET's credibility as a product testing body has been called into serious question.

Having said that, it mu

An Ethical Quandary

Most antivirus companies are under some form of self-imposed restrictions that prevent them from knowingly creating new viruses or virus variants. In addition, competent testing and certification bodies such as ICSA, Virus Bulletin, Secure Computing, and AV-Test.org, do not create new viruses or virus variants for testing.

Indeed, the consensus throughout the antivirus development and testing community is that creating a new virus or variant for product testing would be very bad „ and totally unnecessary. To do so would undoubtedly raise questions about their ethics.

Whether or not CNET knew this fact is unknown, but they did in fact create two new virus variants for

their testing. Please note this fact as described in the "How We Tested" section.

We scanned for the I Love You virus in three different ways. In the first test, we left the code as is. In the second test, we changed every reference to love in the code. In the third test, we changed the size of the file by inserting a comment that did not affect the code.

Changing an existing virus results in a new virus. If a testing body does this, they brand themselves with, as it were, a scarlet "V" (as has CNET at this point). They mark themselves as a virus creating organization in the eyes of antivirus experts worldwide.

More importantly, producing new virus variants creates an incredibly complex quandary. It places the tester in a very difficult position, which can quickly escalate the problem.

When a tester claims that a product should not be purchased because it misses viruses, that tester takes on the burden of proof. Their claim can be challenged. Antivirus companies have every right to demand proof that the testing was fair. If in turn the proof cannot be given, they have the right to advertise that fact and demand a retraction.

Proof generally involves either having an independent body repeat the testing, or providing copies of the viruses missed to antivirus companies. In either case, where the virus was created by the testing body, they would need to send the new virus to someone else. If they send it to an antivirus company, other companies could rightly demand copies, too. But what happens if they send their new virus to someone else?

Creating a virus for testing is one thing, distributing it is quite another. Doing escalates the problem and virtually destroys the testing body's reputation. This is because they then become a virus creation and distribution organization and, once the virus has left their control, there is the possibility that their new virus might escape into the wild and spread.

True, CNET, or some other testing body, could conceivably attempt to sidestep this issue by saying they will not send the viruses they created. They could offer to explain how the antivirus company or independent tester can create the virus themselves, to see why a product missed it. This ploy is obviously not a solution, because ethical tester organizations and researchers at antivirus companies will refuse to create a new virus. In fact, many would also refuse to accept a newly created sample as well.

Contradictory Combination

We've discussed two factors, the use of simulated viruses, and the creation of new variants. If we combine these factors the results produce a contradiction in the logic upon which CNET's methodology is based.

We can ask, why didn't they just use real, common viruses in testing?

The common reason given to justify the use of simulated viruses is the possibility that real viruses

might escape from the test environment and spread. But if this was CNET's reason for using simulated viruses, wouldn't the same possibility of escape have existed for the two viruses they created. Or is the opposite true? They might have had a good, secure environment in which to test their new viruses. But if that's the case it only brings us back to asking why they didn't use real viruses in that same, safe environment.

Each of these two factors (using simulated viruses and using modified viruses) has been demonstrated as an invalid basis for testing. When we juxtapose these two factors we evidence our claim that the logic underlying CNET's methodology is contradictory, further weakening the already-crumbling foundation upon which their "virus testing" was based.

Summary

The use of simulated viruses in CNET's review is bad. Representing them to readers as "test viruses" is worse. But creating new virus variants is the worst transgression of all -- especially as such tactics in testing are totally unjustifiable. There are better ways to test.

Well-documented methods to effectively test various antivirus solutions are available. Several excellent papers exist on antivirus product testing. There are also competent antivirus testing labs that can provide metrics testing, which can be fully documented and easily reproduced.

Moreover, it cannot be claimed as a matter of cost. Some antivirus labs test a variety of products on a regular basis and permit the publication of their most recent test results at little or no cost. Why do they do this? Because, first and foremost, they desire to see the publication of high quality, incontrovertible test results, rather than misleading results based on questionable methodology.

As a result, there is absolutely no justification for the use of simulated viruses, which do not represent reality. There is never a reason to create new viruses to test products, especially when there is not a secure, dedicated virus testing facility.

If CNET does not have a secure virus test lab then they should use a competent outside lab. Other news organizations do so. Indeed, there are highly qualified testing labs that can do accurate testing against viruses and under conditions that reflect reality.

Therefore, we must conclude that, when reviewing antivirus products, statistical metrics involving viruses should be delegated to antivirus experts who do it all the time. At the same time, other product facets such as usability, intuitive interface, update issues, support factors, and so forth should by all means be done by the experts at CNET who regularly test a variety of software. This methodology will solve the problems encountered in CNET's antivirus product review of September 21, 2000.

It is therefore hoped that CNET, as the responsible news source it is, will retract the entire test, renounce forever the flawed methodology, and provide fair, factual, and beneficial antivirus product reviews in the future.

Maybe the four products tested by CNET would score exactly as they did in the fallacious testing or

maybe they wouldn't. But in either case, the product review would be based on facts rather than falsehood. Thus CNET's readers would benefit, instead of having their trust betrayed.

Sincerely,

Joe Wells

CEO and Director of Wells Antivirus Research Laboratory, Inc. USA CEO, Founder and Director of WildList Organization International Former Senior Editor of IBM's antivirus online magazine, USA Advisory board member Virus Bulletin, UK

æ The following individuals have asked to have their names attached to this open letter to indicate their agreement and support in this matter.

Francesca Thorneloe
Editor of Virus Bulletin. UK

Pavel Baudis
Vice President of ALWIL Software, Czech Republic
Advisory board member Virus Bulletin, UK

Kenneth L. Bechtel
Founder of Team Anti-Virus, North America

Dr. Vesselin Vladimirov Bontchev
Antivirus Researcher at FRISK Software International, Iceland
Founding member of CARO (Computer Antivirus Research Organization)
Founding member of VSI (the Virus Security Institute)

Shane Coursen
Manager of WarLab virus and antivirus testing facility. USA
Vice President of Wells Antivirus Research Laboratory, Inc. USA
Directf WildList Organization International

Joost De Raeymaeker
Owner of RSVP Consultores Associados, Lda. Portugal

Allan Dyer
Chief Consultant, Yui Kee Computing Ltd. Hong Kong

Nick FitzGerald
Director, Computer Virus Consulting Ltd, New Zealand
Advisor to the WildList Organization International
Former editor and antivirus product tester, Virus Bulletin, UK

David Harley

Security Analyst, Imperial Cancer Research Fund, UK
Consultant, SherpaSoft Anti-Virus UK & Mac Virus UK

Dr. Jan Hruska
Chief Executive Officer, Sophos Anti-Virus, UK

Jose Martinez
Manager of Hacksoft S.R.L. Perce

Andreas Marx
University Otto-von-Guericke Magdeburg
Head of the Virus and Anti-Virus Test Lab "AV-Test.org", Germany

Petr Odehnal
Head of Virus Lab at GRISOFT(c) SOFTWARE, Czech Republic

David Phillips
Project Officer, The Open University, Technology, UK

Peter V. Radatti
President and CEO of CyberSoft, Inc., USA

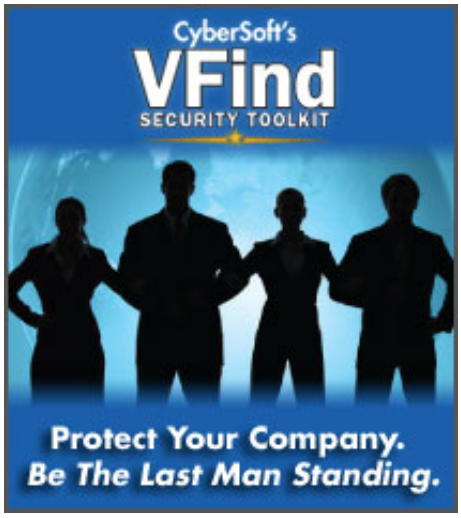
Stuart Taylor
Head of Virus Laboratory, Sophos Plc. UK

Robert Vibert
Anti-Virus Researcher and Solution Architect at Segura Solutions Inc. Canada

Eddy Willems
Technical Director of Data Alert International, Benelux
News Editor for EICAR

Righard J. Zwienenberg
Anti-Virus Researcher at Norman ASA, Norway
Founding member of VSG (the Virus Strategy Group)

Representatives of Aladdin Knowledge Systems, Network Associates, and Trend Micro, regret their inability to be signatories, as their products (eSafe Desktop, McAfee VirusScan and PC-cillin 2000) were included in the review.



508 Compliance TestPros TESTED

This site certified 508 Compliant