# COMMENT

> “ Viruses and other malware could break the Internet even with all the filtering software in place. ”

## Viruses: Is the Battle Really Changing?

There is a lot of gossip these days about computer viruses. If you go to a seminar about *Microsoft*’s *.NET* framework, or to a presentation of *Canon*’s brand new digital camera, it seems that everybody is talking about computer security and viruses. On the train, at the airport, everywhere I go I hear people talking about it. Everyone seems to be an anti-virus expert. However, if you listen carefully, you can overhear the most ridiculous statements, ranging from: ‘If you are not connected to the Internet you can’t get viruses!’ to ‘My firewall should block all the viruses I have, but still I’m spreading Klez and Bugbear … strange!’. Here are some of the statements I have overheard:

‘*Gateway protection was not needed and didn’t exist 15 years ago!*’ Let’s go back to the year 1988. If you had a good anti-virus policy at that time you probably worked with what we called ‘sheep-dip’ PCs. These workstations, positioned in strategic places, were there to scan every incoming document, spreadsheet and program on diskette. This was the ‘Gateway’ protection *avant-la-lettre*. Anybody who says that this kind of protection didn’t exist years ago is wrong. Email was rarely used in those days and certainly not in the format we know it in today.

‘*The EICAR test string is going to change, and that will be a problem for detection of the old string*.’ The string itself will not change. The string remains the same as it was in the early 1990s. It is the definition that will be changed slightly from 1 May 2003. The change is in order to make it impossible to include the EICAR test file within any virus and to make it easier for any anti-virus vendor to detect it as the unique EICAR test file. More information will be provided at the EICAR conference this year and on the EICAR website (http://www.eicar.org/).

‘*The virus battle is changing!*’ Is this really the case? From some of the poorest people to presidents and royalty, almost everybody is using the largest network in the world: the Internet. And, as a result, everyone gets viruses, spam, chain letters, and so on. We already have three times more spam than last year and it’s still on the increase. So, as the Internet ‘matures’, governments, corporations, universities and service providers are erecting fences.

The Internet worked well when computers did no more than their assigned roles: pass along data packets to the next computer. Now those computers, in control of several parties, are increasingly being called upon to make social judgements: is that packet advertising, pornography, a virus or terrorist communication?

Of course, without content filtering in the workplace, employers lose productivity and risk lawsuits if workers access illegal material. But the fight against junk email sometimes backfires – legitimate mail such as newsletters for support groups is sometimes blocked mistakenly, often without senders or recipients knowing. Other barriers are also on the way as wireless access becomes more common worldwide.

So, if you look very closely, you can see that there is indeed a change in the battle. Spam is just one problem. Unfortunately, it’s not the only one. That’s one of the reasons why the anti-virus industry is making moves to include firewalls, anti-spam and other security breach detecting techniques in their products. And it’s not only the anti-virus industry who seem to be starting to bundle everything. Within the new era of *.NET*, *Microsoft* is gathering everything together to make it more user-friendly. Look at the W32/SQLSlammer worm or W32/Nimda or W32/CodeRed or even W32/Klez. What if virus writers start to combine their techniques too? What could happen if the virus writer combined some DDoS attacks with a worm which sent out spam and made the payloads more dormant and then the AV industry overlooked it for, let’s say, a few days …

Is this fiction? I don’t think so. Viruses and other malware could break the Internet even with all the filtering software in place. It nearly happened last year (attack on the 13 DNS root servers) … will it happen this year?

*Eddy Willems, Data Alert International, EICAR Director Information & Press, Belgium*