Virus Trends 2003-2004

Computer Viruses have come a long way since the Brain Virus first infected floppies way back in 1986. The W32.Netsky.B mass-mailing worm, released in February 2004, is a classic example of the distance virus technology has traveled. Netsky arrives in email, and once it infects the computer, searches for all email addresses it can find on the PC, and sends itself to them, using its own mail server engine! For good measure, it disguises the sender's address, so the source cannot be easily traced, and also copies itself to as many shared drives that it can find. The subject line and contents of the infected mail are not constant and change from infection to infection.

This single virus, or worm to be precise, incorporates several virus technologies developed in the last decade -

- Stealth or hiding itself to prevent easy detection
- Polymorphism or changing each instance of itself, to make signature development difficult,
- social engineering - tricking the user to activate the virus by some innocuous but interesting message
- mass-mailing – transmitting itself to mail id's on the infected user's PC without his knowledge
- Blended attacks – using a combination of attacks to exploit vulnerabilities spread to the maximum number of computers in the minimum time

2003 in fact was probably the one of the worst years in terms of havoc wreaked by viruses. Slammer in January, Bugbear in June, Blaster and Sobig in August – it seemed that one took off where the other stopped. Why is this happening, and on such a big scale? The second question is easier to answer. The widespread use of networks and Internet have made it possible for a virus to infect a million hosts in a matter of hours. One theory that attempts to answer the first question is that it is a cat and mouse game between virus authors and anti-virus companies, each trying to outwit the other. But that is only part of a bigger story – viruses and worms spread because there are vulnerabilities in the underlying Operating System and Networks itself. Some of these are inherently insecure. Unless these issues are fixed, someone or the other will try to exploit them for his or her five minutes of infamy.

What can we expect for 2004? More of the same, for starters. On the technical front, many new techniques are being used by virus writers –such as de-activating anti-virus software, spreading via peer-to-networks etc. But more worrying is the change in motivation underlying the problem. Earlier most virus writers were teenagers trying to show off their computing skills in peer groups. But now viruses and worms are displaying more sinister reason – crime and financial gain. Users are being prodded for credit card, bank account and social security numbers, usernames, passwords and other sensitive data. Identity theft is not a storybook scenario anymore. People's confidential identification information are being stolen and used to buy products and services that are then sold off to third parties for financial gain.

While the virus problem can never be completely eliminated, several steps can be taken to minimize its impact. At the corporate level, an appropriate computer security policy has to be defined and implemented to catch the the problem as early as possible. This would consist of policies, procedures, products and services. Good anti-virus software, updated almost on a daily basis, has become a necessity. Some integration with Firewalls and Intrustion Detection Systems would also help to handle the new blended threats that are coming out. Spam mail, besides being a nuisance, is also a common source of viruses and needs to be dealt with at the organisation level rather than at the end user level. Network administrators need to keep themselves abreast of new vulnerabilities and exploits that are being detected and ensure their systems are patched to be protected. Large organisations need to look at some patch management solutions as well. Periodic audits are required to ensure that the policies and procedures and being complied with and review of the policy every 3-6 months or so ensures it is uptodate. An effective backup and disaster recovery system is a must, since no protection is fool-proof.

At the end user level, a lot of education is required. Users must be told to ensure their anti-virus software is active and up-to-date at all times. Under no circumstances should they be allowed to disable it. They should be instructed not to open attachments in emails from unknown persons – or even from known persons unless they have requested it or specifically know what is inside. Spam mails should not even be opened at all. Browsing at non-business sites should be discouraged not just for the productivity losses it causes but the possibility of picking up virus infection along the way. Home users who connect to the office network require extra protection – especially since the kids at home will also be using the PC for several other purposes!

To conclude, viruses and worms are here to stay. It is upto us to ensure that they do not unduly interfere in our business and cause us losses. As in all cases, an ounce of prevention is worth a pound of cure!