Network Virus Protection Strategies

by Dr. Frederick B. Cohen ‡

An article for Netware Solutions

‡ This research was funded by ASP, PO Box 81270, Pittsburgh, PA 15217, USA

Computer viruses 'infect' other programs by modifying them to include versions of the virus. With this infection property, viruses spread from program to program, from computer to computer, and from network to network, causing corruption, leakage, denial, and evasion as they go. Let me give you an example:

One nightmare scenario I encountered fairly recently involved a Novell network in a phone room used for handling incoming 800 and 900 number calls. They called me at 4AM explaining that at 8AM, they would have hundreds of employees unable to answer the telephones unless they could eliminate the virus from their system. The virus apparently spread through their network unnoticed over a matter of weeks, and restoring from recent backups would, at best, only delay the problem. Widespread denial of services was taking place, as many of the infected programs would no longer run.

There are hundreds of virus defense products in the world market, with prices ranging from $2 to over $200 per copy. With this much range, it's hard to figure out what to buy. To really make a good decision, you should read a good book on viruses. A good book is 'A Short Course on Computer Viruses', ASP Press, PO Box 81270, Pittsburgh, PA 15217, USA), but here are a few basics about virus defense in LANs and how to make your decision.

There are three kinds of defenses on the market today.

- Sound defenses work today, and will work for the forseeable future. The **only** sound and practical defense today is limiting information flow through access control. Access control can be used to protect the virus defense from attack, and is a vital component of modern virus defense, because a defense that can be corrupted is vulnerable to modern 'stealth' viruses. In modern networks, access control management can be quite complex, and requires tools beyond those currently available. For example, a typical Novell network has on the order of 100,000 files, each with about 10 protection bits, for a grand total of 1,000,000 protection bits.

- Solid defenses work today and will work for some time to come, but they can be bypassed by a clever enough attacker. The most cost effective one is the 'Integrity Shell', which uses cryptography to 'fingerprint' information and verify the fingerprint just before use. The best integrity shells are fast, automatic, and transparent. They automate repair, take under 4K of resident memory, operate on LANs, and protect against all sorts of corruption, including known and unknown viruses. The most sophistocated LAN based integrity shells even perform network based backup and recovery at runtime, and automate some aspects of LAN management.

- Weak defenses are ineffective against many current viruses, are expensive to use, and are usually designed and implemented in a very short time with very little thought put into them. The most common one is the 'virus scanner' which scans for known

viruses at bootup. The major problem with scanners is the wasted time and expense associated with periodic scanning and updates. They are also ineffective against many 'stealth' viruses. The best of the weak defenses is a 'virus monitor'. Monitors catch known viruses at program load, which eliminates the slow bootup checks, and prevents known viruses from ever being run. It doesn't solve the update problem, and with more than one new virus detected per day, you have to update very often to keep up with the times.

Things to look for:

Look for products that have been around for several years. Many virus defense companies go out of business in a year or two, leaving their customers out in the cold.

Look for companies with well known computer security experts. A good defense is hard write, and most newcomers are out of their depth. They write defenses that will ultimately fail and cost you a fortune.

Look for integrated products that combine all three types of defense to give 'defense-in-depth'. Over a two year period, they will be more effective, and cost less to operate than their cheaper counterparts.

Things to avoid:

Products that claim to catch **ALL** viruses. This is not a credible statement.

Products with misleading ads. One company claims to have the **only** LAN compatable defense - it's not true! Remember that you are trusting your supplier to protect the integrity of your information. If the ads don't have integrity, the products probably don't either.

Don't be fooled by the number of viruses detected. According to IBM, a scanner that detects the 40 most common viruses catches more than 95% of all attacks. Scanners that look for hundreds of viruses often miss some of the most common ones.

At runtime, pop-up windows and graphic logos waste time and space and distract users from their work. The best defenses only flash a small message on the screen at runtime. Attacks are quite rare, but the waste caused by the defense is ever-present.

Several 'name brand' products are poorly designed. Some well known companies rushed to get products on the market and spent big bucks on advertising, but they sacrificed quality and good design for fast delivery.

A Final Note:

Viruses are here to stay. The time you spend learning about them and searching for the best product for your environment is time well spent, but don't wait till your network gets

infected to make your decision. I've repaired far too many networks that never should have been infected. An bit of prevention is worth a gigabyte of cure.

ABOUT THE AUTHOR: Dr. Cohen is widely considered the world's leading expert on computer viruses and virus defenses. He invented most of the defense techniques in widespread use today, and won the international "Information Technology Award" in 1989 for his work on virus defenses.