

Redefining e Security

By Govind Rammurthy – CEO and MD, MicroWorld Technologies Inc.

“Every new technological leap will be subverted by perverse minds”. A wonderful boon like e-mail, which connects people across time zones, very economically, has now become a source for viruses. The Internet, which brings the whole world to your PC, has now become a scourge, with pornography and other despicable acts, defiling the sanctity of your home and organization. Your trusted employee may e-mail confidential data to your competitors. The list grows and so does our paranoia. Names like Love Bug, Melissa, Klez, etc. are voraciously and morbidly read by people across the globe. The headline ‘New Virus appears’ is sufficient to send the masses into a tailspin. There is a sudden spurt in buying Anti-Virus products, the virus is nullified and then the world waits in trepidation, huddled in terror and waiting for a new one to strike.

There is another type of threat, which **kills** your organization, rarely makes dramatic headlines but is always omnipresent: confidential data e-mailed by an employee, abuse of a productive tool like the Internet, Spam, offensive mails etc. The losses run into billions, lost opportunity costs - incalculable.

Can we hope for a safe computing world? How do we ensure that viruses, unsolicited and offensive mail, etc; do not enter our home or organization? How do we ensure that our confidential data is not sent to our competitors?

In this article, I will try to explain how it all started, different types of viruses, how they attack, how Anti-Virus products work etc. I will also tell you about a radical concept, **MWL**, which takes the fight into a virus author’s backyard.

Virus – Brief History

In 1981, **Elk Cloner**, a computer program which infected Apple II floppies appeared. It displayed a rhyme “It will get on all your disks, It will infiltrate your chips, Yes it's Cloner!”. Then in 1986, Sajid and Amjad replaced the executable code in the boot sector of a floppy, with their own program. Over the years, the virus evolved to keep pace with changing technology. The year’s saw viruses like stoned, Aids, Jerusalem, Michelangelo etc, appear. Virus changed forms and we have types like: self-mutating, polymorphic virus etc. While the first few viruses took almost three years to spread across a few organizations, the Klez worm spread across the world in 22 minutes!

How viruses attack

Each virus has a specific destination and method. The method of attack is defined by its type. Some types are explained below:

Boot Sector Virus - Places its code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus lodges itself in the PC memory and gains control over the PC. From here it spreads to other drives on the system.

Polymorphic Virus - Creates varied copies of itself to avoid detection from anti-virus software. Some use different encryption schemes and require different decryption routines. So the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands to mislead anti-virus software. Some use mutation-engines and random-number generators to change their virus code and decryption routine.

Self-encrypting Virus - Conceals itself from anti-virus programs. Most anti-virus programs attempt to find viruses by looking for certain patterns of code (known as virus signatures) that are unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection.

Stealth Virus - Conceals its presence from anti-virus software. Many stealth viruses intercept disk-access requests, so when an anti-virus application tries to read files or boot sectors to find the virus, the virus feeds the program a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection.

File Virus - Replaces or attaches itself to COM and EXE files. It also infects files with extensions: SYS, DRV, BIN, OVL, etc. They can be resident or non-resident, the most common being resident or TSR (terminate-and-stay-resident) viruses.

Mutating Virus - Changes or mutates as it runs through its host files. Disinfection is more difficult.

We have many sub-class of virus: Macro Virus (infect Word and Excel files), AppleScript Worms, BatchWorm, etc.

How are Viruses detected and removed

Wish I could answer this one easily. At MicroWorld Technologies Inc, we have a well-equipped lab, where the virus is 'dissected' or disassembled with a disassembler into its components. This is a skilled job and requires experience. Extensive knowledge of DOS programming, assembly language, C/C++ etc, very detailed knowledge of operating systems, etc. is a must. We run the virus on our machines under controlled conditions. Once we have the detailed mappings in place, the next task is to reverse engineer and find a way to reverse the effect. Ultimately a vaccine is produced. This process can take anywhere from two minutes to two days. Detection and scanning is a cat and mouse game. Actual detection in your machine is done through by: Reference scanning and Heuristic scanning.

Reference Scanning:

Known viruses are recognized by their structure called virus signature. Almost all Anti-Virus software's have a database with details of known viruses. The software checks files and folders for such virus signatures, detects and removes it. But every month about 500 new viruses are 'released'. These are detected using heuristic scanning.

Heuristic Scanning: Virus infected files display strange behavior, form, content or have strange code. Good Anti-Virus software's have the ability to 'feel suspicious' about such files. Users are immediately alerted about such files and depending on the options available, they delete or quarantine them. Products like **eScan** and **MailScan** have a very high level of heuristic scanning capability. They allow the user to configure the application to automatically quarantine such files and even e-mail a copy of the file to us for analysis!

Pre-emptive strike

The focus always has been on detecting and removing a threat, **after** it has infected the system. Our **MWL** (MicroWorld Winsock Layer) technology, addresses threats from a new perspective. When you connect to the Internet, you do so through the Windows Socket (Winsock) layer. It acts as an interface between your computer application and the Internet. It does its work very efficiently and you can surf the net, download programs, etc. unhindered. But it never distinguishes between a virus infected file and a clean one. It never stops unwanted mails or your confidential data from entering or leaving your organization

The **MWL** (copyright pending) layer sits on the Winsock layer. It checks and analysis all traffic between your system and the Internet. All e-mails, attachments, downloads, uploads, etc., mandatorily pass through MWL before they enter or leave your system thus providing you a secure blanket.

You now have a secure MWL net through which all traffic must pass. Our applications, which are based on this technology, have built in features that scan the traffic for viruses, Trojans, Worms etc, detect and remove them. Now comes the tricky part of providing content security.

CONTENT SECURITY

You may have received offensive mails, perhaps with content, which deeply offends your sanctity. A trusted employee may be e-mailing confidential data to others. Content security ensures that all traffic entering or leaving your system conforms to your security policies. You can specify that incoming and outgoing traffic shall not have:

- Words or phrases like xxx, naked etc. Any mail, file, compressed file etc, that has such words, anywhere in it, will be stopped before it enters your system. (In fact, I had to ask my system administrator to allow this article to be e-mailed, as we have a security policy, which bars these words!). You can trace the source machine, which indulges in these acts.
- File with extensions like .exe, .doc, txt, etc, or above a certain size, shall not be allowed out or into your organization.

Our products are built on the MWL concept. All the above tasks are done in 'real-time', as the event is occurring. In fact, it is the MWL concept, which has made us the leading provider of Content Security and Anti-Virus solutions.

MicroWorld's Products

We have two product suites: eScan and MailScan.

eScan: eScan is an 'enterprise-wide, 'Anti-Virus software that scans your local and network drives and TCP/IP traffic for viruses and cleans them on "real-time" basis. There are five individual products in this suite.

MailScan: MailScan the world's first 'real-time', Content Security Software for corporate **mail servers**, that performs content filtering and virus scanning of **mail servers**. There are 17 products, each designed for a specific mail server.

Just in parting "Remember, virus authors are perverse but brilliant, with access to advanced tools. Rely on MicroWorld products to beat them".

Govind Rammurthy can be reached at govind@mwti.net.

For more details visit <http://www.mwti.net/>