# Communicating With Sam

## Microsoft Security Vulnerabilities: Avoidance is not a Strategy

*Sam Johnston*

### Question

Our business lost some productivity earlier this month due to the ZOTOB worm infecting some PCs and Servers. Currently our business infrastructure is the iSeries for business applications and Microsoft servers and PCs for office productivity applications including mail. We do have a LAN extension Internet connection and permit users to browse the Internet and use this connection also for hosting web and for our email. We have a small IT staff with a single server and desktop person and we find it difficult to keep up with all the patches and management of patches on the system. What can I do to make my Microsoft and iSeries environment more secure from these threats?

### Answer

With the ongoing onslaught of attacks against the Microsoft world, many of us wake-up each morning enjoying a relaxing first cup of coffee giving thanks to the wisdom of selecting the AS/400 as our mission critical platform, and for having the good sense to stick with it as it evolved to the iSeries platform. Those that know firsthand the virtues of the iSeries pity those easily swayed that followed the path to Microsoft as a single open standard in a connected world. Of course the enjoyment of that first cup of coffee gives way to indigestion the moment your pager or Blackberry starts chirping and you take that first message from your Help Desk. We all know the drill. All the users called in that the iSeries is down, and having survived the stress of the initial diagnosis, the real issue is that another worm or virus has infected your network, your service provider's network, all your customer's networks, and all of your supplier's networks. The iSeries is idling minding its business, while the entire connected world cannot exchange a packet of value. You may have resisted the Microsoft world, but it cannot be avoided, which means like it or not you have to manage it.

So let's look at the practical reality of what you need to manage in the connected world no matter what platform hosts your mission critical applications. First, to address the process of managing and securing the Microsoft environment there are essentially two fundamental issues. The first issue is managing the patching of servers and PCs and the second is using tools and point products to defend against viruses and worms.

Most security vulnerabilities, worms and viruses come after a Microsoft patch has been released when the virus or worm is able to infect PCs that haven't been updated yet due to the lag in execution. There is the additional challenge on servers and PCs of validating the patch for interoperability with applications, plus the test and acceptance time required to publish patches into your business. Finally, the process of patching local and remote offices can be time consuming and cumbersome to manage. Ultimately lags and gaps are created that can be exploited. However, in light of all these challenges there are products that are designed to simplify and help manage and automate the above processes that can help to ensure that you are protected by minimizing the reaction time to known viruses or worms. However, remember, this is not enough as some security viruses or worms may be created before a vendor patch is released, that could exploit unknown issues and have the same damaging effects. This is why you must also consider the tools to help mitigate the problems.

Server and PC Anti-virus software is a well-known tool to help manage the spread of viruses and worms. However, often times the virus is spreading before the signatures are available and it is a race to download and apply updates. Having a good process and minimizing that lag between availability and deployment certainly is a benefit in most situations. Installing anti-virus software on the host system has the additional benefit of protecting from within as well as from external attacks. There is no need to go into further detail here on anti-virus software as solutions have been common for some time, and most network managers or system administrators are familiar with the technology.

There is a wide range of other products and technologies that can help in managing your environment, including:

- Host based IDS (HIDS)
- Firewall with IDS/IPS as perimeter protection
- Intrusion Detection Systems/Intrusion Prevention Systems internally to support control of infection spreading
- Admission Control technology to validate compliance of host pre-network connection (VPN, LAN)
- Anti-X (Malware, Virus, Worm) Support Servers within the mail forward, browsing domain

Host based IDS works by applying a software tool onto each Microsoft Server and workstation to protect the device from being infected. For example, the Cisco CSA product protects a client from a Day 0 attack by securing the PC and access to the resources on the PC that worms or viruses must use to get onto a PC. Additionally, this product will secure the PC without any configuration. However, Cisco does have a management utility that enables the centralized control and deployment of policy and also acts as an information centre for events on the enterprise. Just think of this product as having hundreds of information gathering points within your network looking out for unexpected network traffic types. Tie this into a centralized management tool and you are in a powerful mitigation position.

Perimeter firewalls can also provide protection against attacks from the outside that are using ports not permitted in the connection. However, the configuration and rules are typically static and while this device is completely necessary for perimeter security, by itself it is not enough to defend against Anti-X attacks. There are industry products that can provide, in addition to a firewall, an enhanced layer of IDS/IPS protection within the appliance that provides an extra layer of security by providing signature support against known worms, viruses and other rogue attacks.

Intrusion Detection or Intrusion Prevention Systems can be used as a perimeter device or as an internal device to help control and block worms and viruses from spreading. IDS system are typically

# TUG Golf Tournament Makes a Wish Come True

*By Wende Boddy*

On June 22nd this year, the Toronto Users Group our their 17th Annual Golf Tournament at the beautiful Nobleton Lakes Golf club. We had some good, bad, and ugly players enjoying themselves on a fabulous sunny day! We incorporated several charity holes at this event, with sponsors donating great prizes that could be won by throwing money into the pot – with the lucky winners being picked out during the great après-golf dinner. The players and sponsors came through again for us this year with flying colours, and we collected $2415 for the local Bloorview MacMillan Children's Centre! Thanks again to the players and sponsors.


Photo By: Kirk LeMessurier

***Heather Lucknow, Richard Dolewski, Valerie McMurtry, and Wende Boddy***

This is not a great deal of money compared to what it takes to provide the services at the Bloorview MacMillan Children's Centre, but believe me – all monies help – and it is greatly appreciated by the centre. TUG supports this organization in their endeavor to enable children and youths with disabilities or special needs to achieve their personal best.

## New Developments at Bloorview Macmillan

The first speech-recognition software for students with learning disabilities hits the market next month. SpeakQ, developed at Bloorview MacMillan Children's Centre is targeted to an estimated 10 percent of students who have strong verbal skills but struggle to read and write. SpeakQ was designed to be simple – in contrast with other speech recognition products-targeted at high-end users (such as lawyers and doctors) who require a high degree of literacy. For example, in order to train on conventional products, the user has to read text on the screen and speak it back – an obstacle for students with reading problems. "We've redesigned the training interface so that the computer reads out the text and prompts the student to speak it back," explained Fraser Shein, the engineer who led the development team. "It's user friendly and intuitive and allows the student to train independently."

Construction is on schedule for the opening of the new Bloorview MacMillan facility this December, bringing Canada's largest children's rehabilitation hospital under one roof.

deployed in a 'network sniffing' mode where all network traffic is mirrored to this device and if anomalies are triggered based upon signatures than action can be taken to reset the TCP/IP stream, alarm support, and dynamically modify firewall Access Control Lists to block offenders. Intrusion prevention takes the technology further by installing the device inline so that all packets are inspected through the appliance and if signatures or behaviours are met then the device can block the packet from moving through. Various vendors have products that work in similar and different ways to achieve this result. These devices are best deployed in the perimeter and within the core distribution aggregation to identify and control the spread of viruses and worms.

Network Admission Control (NAC) technology from Cisco is designed to be proactive by querying the client prior to connection via LAN, VPN or other form of connectivity that will ensure that the client has been setup with the appropriate versions of software and patches and anti-virus from select vendors (research the Cisco.com website for more detail). If a client is not in compliance they are denied access or forwarded to a remediation network to download the necessary patches. This tool can help control introduction of viruses and worms by ensuring that the client is conforming to the corporate standards. This tool will require an investment in time to manage properly.

Anti-X Servers are commonly deployed in the DMZ for browsing and mail forward control. These devices can be used to control the introduction of worms into the enterprise, but must be kept up to date with signature-based technologies.

The iSeries specifically has two related issues that need to be managed: first, alterations to IBM digital signatures or patched IBM programs, and; second, the IFS, which can house viruses. While some modifications to IBM programs may be legitimate, managers need a tool to monitor changes in IBM digital signatures to determine if they are appropriate. Traditionally external PCs have been used to scan the IFS for viruses. However this solution presents serious concerns. In a PC scanning scenario the PC itself can become a backdoor to the iSeries by exploiting the vulnerability of the PCs Windows operating system. The PC scanning method may not detect all viruses in the IFS unless very specific IBM processes are used. This process also requires the use of Netserver, which has such poor performance that most users don't scan the entire IFS generating a false sense of security. The PC scan method is also recorded as a change to the file and adds to time to backup the IFS through the use of the SAVCHGOBJ command. Given these risks, the best solution for your iSeries is achieved through a native iSeries application that can detect alterations or patches to IBM programs and IFS viruses. The solution will automatically update with the latest signatures, minimizing exposures and network workload.

Ultimately, there are numerous solutions that can be deployed from many specialized vendors, each adding an additional element or layer of security. However, this in itself can add extreme complexity, which could actually lead to vulnerability due to unruly management. It is important in trying to minimize the management of the multiple systems to look at products that can provide the most coverage and flexibility, but can also be managed effectively from a centralized location. As an example, Cisco has developed a number of complimentary technologies that are marketed under the Self Defending Network that are effective in managing and minimizing your enterprise exposure through a common platform. This platform can provide an effective base solution, permitting the introduction of specialized products from other vendors when necessary to address specific needs unique to your business. The goal should be strike a fair balance between simplicity in management and robustness in the solution at the most vulnerable points. The only way to ensure that this balance is achieved is to have a strategy that neutralizes the temptation to react to each event with a new solution. While we must react to each event, we must have a proactive framework or we may become vulnerable through our own mismanagement. TUG

***Sam Johnston*** *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com. Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday October 14, 2005.*