COMMUNICATING WITH SAM

Virus Protection: A Code Red Alert for Network Security

Sam Johnston

Question:

The recent Code Red virus scare generated significant concern within our organization. Although it did not impact us, our management are getting increasingly concerned over the regularity of these scares, and the potential impact on our business. Some of us are even longing to return to the bygone days of green screens that could only access the AS/400. Management continues to question whether the business value of applications such as e-mail and Internet access justify the complexity of protecting our mission critical information from threats. However, turning back is not a viable option, despite the attraction of the simpler times when all information was stored and processed on the AS/400. Given this, what strategies do you recommend to ensure we are protected from virus attacks? As well, is our AS/400 immune from these attacks?

Answer:

The mass media attention of viruses like Code Red, and the resulting paranoia that is created within information technology departments and the management ranks alike is indicative of how valuable corporate information has become. The focus of the attention when an event such as Code Red comes along is the destructive and malicious nature of the virus itself; however, it is crucial to not let the emotion of the event overshadow the true business issue. Successful businesses have always been subject to malicious threats, be it physical and now digital. At the root of the fear around virus attacks is the question of whether your network security is adequate for today's digital society.

We discussed overall network security strategy in detail in the March 2001 issue, with virus protection being a subset of an organization's overall network security approach. The key message of this article was the need for an overall strategy for network security that mirrors the approach you would take in considering physical security of your corporate assets. The foundation of this strategy is a layered approach that tries to isolate breaches at the perimeter where damage risk can be mitigated or even eliminated. Of course we also discussed how organizations were as, or even more, vulnerable to internal attacks. Rather than re-tracing these steps, we'll try to give you some tactical suggestions that can specifically address the virus component of network security.

Computer viruses, as the name implies, have a lot in common with their biological counterparts. They spread and replicate quickly, are difficult to eradicate, destroying everything in their path without discrimination. Like biological viruses, prevention and control are the best means to protection from destructive executable code. Battling viruses, both biological and digital, is an ongoing battle, with new and increasingly robust strains occurring daily. The International Computer Security Association estimates that 200 new viruses are created every month. The challenge with both biological and computer viruses is that discovery can come well after the creation, replication and activation phase, and the speed with which researchers can understand and eradicate the virus has a large bearing on the extent of the damage inflicted.

Initially viruses spread primarily by users inserting infected disks into their hard drive. Today the prevalent method of infection is e-mail and network connections to the outside world. As a result, the speed and scope of virus infection has multiplied exponentially. If you are the network manager, or have accountability for information technology security, there is a golden rule: management cannot expect you to pro-

tect them against unknown viruses as there is always a lag between creation, discovery and eradication, but vulnerability to known viruses has no defense. Given that there are no means of eliminating all risk, your goal has to be to eliminate the obvious points of attack.

Viruses come in various formats. Prior to the connected world, the most prevalent viruses were boot sector viruses that infected the boot sector of a floppy disk, spreading to the hard drive and all other disks placed in the hard drive, operating primarily in the 16-bit DOS world. Parasitic or application specific viruses also exist, which reside in memory and infect executable files with extensions such as *.EXE, activating each time the user executes the file. Like boot sector viruses, they also reside largely in the 16-bit DOS world, but some have made their way to other operating systems such as Windows. In the connected world, the fastest growing, and most common virus attack, is the macro virus, which corrupts files associated with specific applications such as Word and Excel. They are not operating system specific, but commonly travel with e-mail attachments, down loads and file transfers. Macro viruses largely attack the Microsoft world, and can be created in languages such as Visual Basic: the abundance of skilled resources with knowledge of these environments has largely enabled the macro epidemic. Trojan horse applications go another step further, in that they are applications that are created primarily to look like something else, disguising the real intent of attack. While the user activates the application based on what it appears to be and is subsequently occupied, the Trojan horse e-mails itself to every user in the user's address book, resulting in the potential for mass destruction. While your AS/400 applications may be largely immune from virus attacks, your AS/400 environment is not. As noted above, most viruses are a result of unethical programmers having access to code and tools that can be turned against legitimate applications.

The spread of viruses is enabled through users being empowered to freely create, share and spread files. IBM has strictly controlled the micro code associated with OS/400, while the programming community is smaller and more easily identified due to the complexity and enterprise nature of most AS/400 applications. The AS/400 world is largely one of granting users access to, and the ability to add to tightly controlled databases, unlike the PC world, which empowers users to create. As a consequence, this has made your core

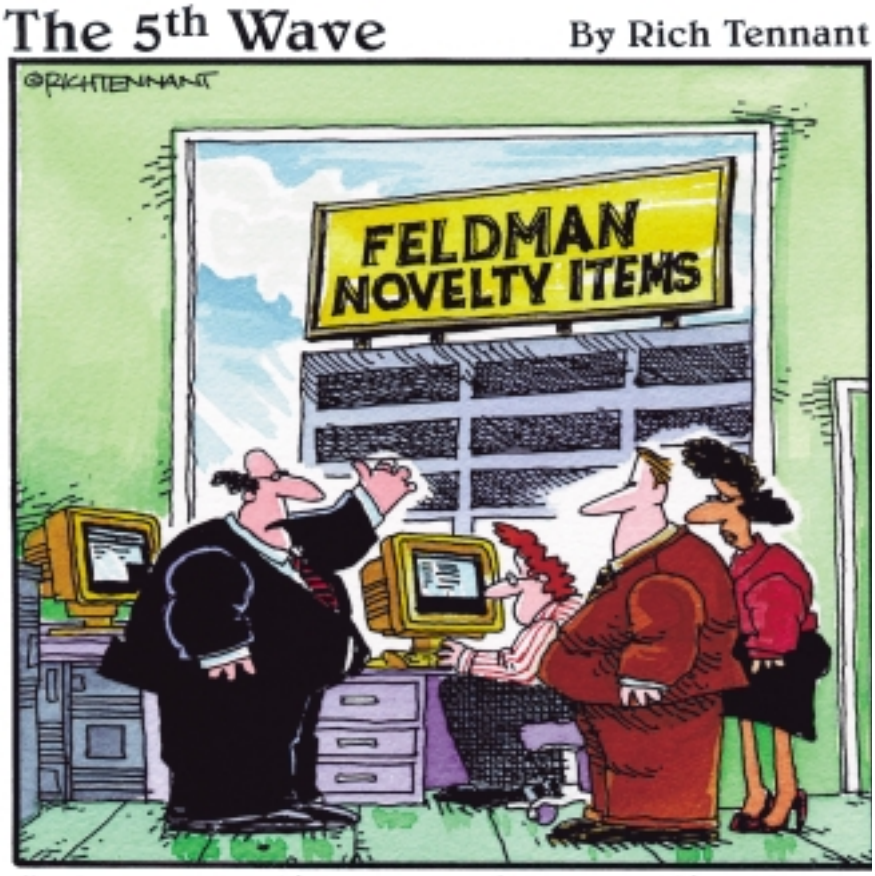
AS/400 applications and databases largely immune from viruses. However, this is not to say that AS/400 access and availability will not be impacted by the macro viruses we constantly hear about. The AS/400 has evolved and can act as a POP3 mail server, or even provide Storage Area Network (SAN) solutions that enable multiple servers, including Intel-based platforms, to share common disk on the AS/400. Further, most AS/400's are now IP-enabled, with users accessing AS/400 applications via the same IP Windows PC network that services applications such as e-mail. As a result, virus attacks that cripple the IP network can impact AS/400 availability.

To adequately protect your environment from viruses, your strategy and tactics need to be layered like your overall network security plan. You need to focus both at the perimeter of your network, as well as on internal resources. At the perimeter, there are a few simple practices that if followed will greatly reduce your vulnerability. First, reduce and consolidate all your external access points ideally to a single Internet connection that has a proper firewall. Eliminate remote branch offices from having dedicated Web connections unless they connect to head office via VPN. Audit your environment to find those renegade departments that demand their own Internet connection. Second, eliminate all those dedicated dial connections to suppliers, customers and service bureaus, and push them via the Internet using VPN technology. If they still require dial-up point-to-point connections, make sure they go via a single controlled access server that controls rights and has accounting tools to diagnose possible breach points. By consolidating your connection points, it is easier to manage policies such as blocking users from visiting unapproved Web sites.

It is also more cost effective to implement tools for screening for viruses. Given that e-mail attachments are a primary source of virus infection from the outside world, it is crucial to ensure that you have the right architecture to screen for viruses prior to their entry into your production mail server. Too often we still see organizations that simply put their production mail server behind a firewall, allowing e-mail from the Web to directly access the production mail server. The assumption is that the firewall will stop all unwanted traffic, but by its nature, the firewall must have ports opened to permit authorized traffic through. A legitimate e-mail still may be virus infected. The correct architecture is to have a mail forwarding server that is hardened and protected via TCP port 25 for SMTP. This effectively means a mail server residing in the DMZ (De-Militarized Zone) of the firewall, which is a network behind the firewall, but external to your production network – a digital reception area. The mail-forwarding server screens in-bound mail for legitimacy. Additionally, if it is designed to support features such as Tight SMTP Protocol and anti-spamming, then the server will also screen incoming mail for viruses.

As a practice, you should also screen outbound e-mail traffic for viruses to ensure you are not contributing to the epidemic, maintaining your good corporate citizen status. Software exists with this functionality, but it needs to be managed tightly. You will need a process to update virus signatures on a regular basis to ensure that you do not become a victim of the latest known virus. You should also implement blocking techniques to alert information technology managers, and importantly

source organizations, of infractions as they occur so you can proactively intervene. With new viruses being created daily, and the lag in discovery, perimeter defense cannot completely reduce risk. However, hardening your server appropriately and ensuring that you apply all the latest security patches in a timely manner, will likely mean that you will be able to protect yourself from the most common threats. As discussed, a layered approach to virus scanning is recommended. Due to lags in discovery of new viruses by the virus scanning software industry, it is completely possible that a virus may get past scanning on your mail forwarding serving prior to an update to the virus signatures. Further, some viruses may mutate and no longer be able to be detected. To protect against this, it is crucial that you run additional virus scanning on your PC LAN network to ensure that once you do update the virus signatures that the scanning software can isolate any infected files that may have slipped through the mail forwarding server. This practice will also protect you from the threat of users inserting disks or CDs into their PCs that are infected with viruses. Of course, the best practice is still prevention. It is crucial that you have tight policies and procedures for your PC network. Effective tactics include forcing users to store all e-mails centrally to reduce the number of source points you need to manage. Although it is hard to police users and prevent them from loading infected disks or CDs, you can reduce their ability to freely act by administratively locking PC devices, or removing and disabling drivers through Windows NT or 2000. It is also important to regularly audit your PC environment to ensure that users are following corporate policies, and make sure that human resources has a code of conduct that clearly defines the outcome should an employee endanger corporate assets. Lastly, only provide a PC where needed, using diskless PCs, or even 5250 terminals, when you can.



In the end, it is nearly impossible to defend against all virus attacks with the speed and volume with which they are created. However, sound virus scanning and network security practices will greatly reduce the risk of common threats and provide you with the tools to act quickly when you do come under attack. These factors will greatly reduce the potential cost of virus attacks to your business. TUG

Sam Johnston *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to theAS/400 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 12th, 2001.*