CRN Vital Information for VARs and Technology Integrators

October 20, 2003

Network & Security Technologies

GUEST OPINION

Ready to Defend the Next Blaster?

Understanding the behavior of your networked business apps

By Adam Lipson

CRN

- 10:31 AM EST Mon., Oct. 20, 2003

As a result of the recent onslaught of Internet-based virus attacks and their effect on many companies' operations, some organizations responded defensively by shutting down TCP ports that were vulnerable. Unfortunately, many quickly learned that other essential business applications relied on these same ports and that they had, unknowingly, shut down critical business applications.

The problem highlights the need for enterprises to understand the functional behavior of existing networked business applications and specifically to inventory their port usage.

The Blaster worm took advantage of the underlying behavior of networked applications to enable its rapid spread. Many other viruses and worms rely on similar vectors of infection. This behavior is based on the underlying common protocol used by all Internet applications as well as those running on most modern corporate networks. This protocol, TCP/IP, transmits data by encapsulating it in an electronic envelope. The envelope bears an address that networks and computers use to route and process it. Just as regular mail addresses can be broken down into functional parts (e.g., street number, street, city and state) so can the TCP/IP address. One of these address components is known as the TCP port.

The TCP port, usually assigned by the Internet Assigned Number Authority (IANA), designates the destination application for the data. It's sort of the street number that the destination computer uses once it receives the packet from wherever it came in the network. Interestingly, network traffic from Blaster and similar worms use a fixed port number (the street number), even if the rest of the address is different (continuing with the analogy, the city, state and street are all different--just the street number remains the same.)

In response to the Blaster virus, a number of advisories recommended that network managers set up blockades against the Blaster port numbers (it actually used a few) to prevent its spread. This turned out to be a problem. The worm used these ports because other software actively uses them. Thus, when the managers set up their blockades they did more than stop the spread of the worm, they stopped the flow of vital data and control communications.

While Blaster slowed traffic (by overloading network connections), the managers stopped traffic completely.

Of course, future viruses and worms will likely contain more destructive payloads. So, stopping their spread is critical. Yet, the question remains: How can network and security managers prevent or lessen the blow of implementing such traffic blocks?

Modifying all network applications to use different ports won't help. Besides, doing so would require enormous effort, and all the worm would have to do is target the new ports. So, something more is required.

If network managers know that a worm or virus always uses the same port number, they could try to key off of something else in the packet, couldn't they?

Unfortunately, builders of malicious software have already thought of this. The generic parts of the envelope--the state, city and street in our analogy--always appear valid. Even if they are forged, there's no way to tell how or what is right or wrong. So looking in the envelope does no good.

Looking into the data or packet payload that contains the worm's executable instructions holds some promise. However, the bad guys have thought of this, too. Most try to hide the instructions through random variations that make it difficult to identify a signature for a particular worm or virus. An effective packet-scanning firewall must constantly receive updates of the very latest signatures to even stand a chance of catching an incursion. With so many to check, the firewall becomes a serious bottleneck. So far, nobody has come up with an efficient way to do this.

This leaves us with no choice but to understand better what passes over our networks, its value and how it operates. In the event of a release of a new worm, network managers can use the port number as a crude blockade, just as before. But, in order to effectively use port blockage, they must first understand what valid applications operate over these ports so that they can make informed allowances.

Unfortunately, few organizations understand the relationship of their networked business applications to port numbers. Sure, it's easy enough for a network analyst to identify the ports used on the network. However, this is of marginal use. It just enables network managers to say to their business counterparts, "I'm blocking port 445, which runs on servers A and B. OK?" Frankly, few people--even the techies--understand what this means to the bottom line.

Associating port numbers with specific machines and the business applications that run on them is something entirely different.

The application/port-number inventory should produce a list of applications with names meaningful to the business. That is, instead of saying "Server A is running NetBIOS over port 135," the inventory should say, "Our internal cash management system, Enterprise*Cash, uses NetBIOS port number on Server A." That makes sense to network managers and security officers who have to watch for malicious codes. However, Enterprise*Cash means something to the finance department. This empowers both sets of managers in the defense decision process. An inventory must also take into account the underlying applications that support the networked business application, such as operating systems, databases and a firewall that all reside on the same server and that all require TCP ports.

Such an inventory requires a much more involved process that relies on both technical and non-technical methods. But, through this endeavor, businesses will understand the business impact of implementing defensive network access controls, such as those recommended for the Blaster Internet worm incident, against future attacks.

Eventually, CIOs will require this type of application/port-number inventory. It's just a wise business practice, not unlike maintaining well-indexed customer files. In so doing, they might not prevent the next Blaster, but they will make sure to minimize its effect on their operation, and thus the bottom line.

Adam Lipson is president and CEO of Network & Security Technologies (www.netsectech.com), a leading provider of digital security consulting solutions based in Pearl River, N.Y. He can be reached at adam.lipson@netsectech.com