Viruses have become much more destructive than ever before by combining or blending a number of dangers together. The CodeRed and Nimda worms are examples of these new kinds of blended threats. Learn what you can do to protect your company’s data against blended threats.

The Blended Threat: Preventing Computer Security’s New Nemesis

By Cosmo Battinelli

IN 2001, the computing community was introduced to a new kind of threat—one that could pick and choose its point of entry based on the security roadblocks it faced.

This new nemesis brought with it a number of unexpected and extremely sophisticated dangers. According to Computer Economics, an independent research firm in Carlsbad, CA, the worldwide economic impact of malicious code was $13.2 billion in 2001 alone.

THE NEW NEMESIS

The first known computer virus appeared in 1981, a relatively tame outbreak by today’s standard, that required users to physically transport an infected disk to another computer for the virus to spread. Today, however, viruses have developed into much more.

These new threats combine to create a modern type of advanced computer security threat that experts are calling “blended threats.” As the term blended threats denotes, these threats combine, or blend, a number of dangers together into one destructive force.

The Code Red and Nimda worms were examples of these new kinds of blended threats, both of which invaded millions of servers and PCs within hours and will continue to harm for years to follow. The Code Red worm was a major shock to the antivirus industry since it was the first worm that spread not as a file, but solely in memory by utilizing a buffer overflow in Microsoft IIS. Nimda was nearly as devastating, as it was set up to insert malicious code into executable files, change account privileges, reconfigure network shares, make registry changes and inject script code into HTML files.

These exploits, vulnerabilities and buffer-overflow techniques have been used by malicious hackers and virus writers for a long time. However, until recently, these techniques, as well as others listed below, were not commonplace in computer viruses.

Multiple methods of propagation

The very nature of a virus is that it is self-replicating—once released, it propagates on its own. A blended threat is a security threat that uses multiple methods to attack. Some propagation methods include being embedded into HTML files of an infected server, infecting any visitors to a particular Web site, and even sending e-mails with a worm attached. Multiple methods of propagation can make containment of a threat an even greater challenge.

Multiple points of attack

Blended threats attack on multiple levels, while simple viruses spread by attaching a copy of itself to some part of a program file or record. By striking on several levels, it makes these threats extremely difficult to detect and especially difficult to clean up.

Spread without human intervention

Blended threats are automated, continuing to spread without human intervention. As a result, they are always scanning the Internet for vulnerable servers to strike. This increases the danger, as they are automated, and makes them much more challenging to halt.

Exploits vulnerabilities

One of the most dangerous aspects of a blended threat is that it can exploit vulnerabilities.

Typically, blended threats abuse known vulnerabilities such as buffer overflows, HTTP input validation vulnerabilities, known default passwords and others. A buffer overflow occurs when a program attempts to store data into a buffer, where the data is larger than the size of the buffer. The ability to exploit a buffer allows one to possibly insert extra code into the execution route. Hackers find the holes within a network and hit where it is least expected.

Causes harm

Unlike some worms and viruses, blended threats are built to be destructive in nature. Some attacks have been known to launch a denial-of-service attack at a target IP address, to deface Web servers and to leave Trojan horses behind for later destruction.

By combining these characteristics, blended threats have the potential to be more harmful and deliver more damage than the typ-
itical virus or worm. Security exploits are being combined into intricate computer viruses, resulting in a very complex attack—a blended threat—that in some cases goes beyond the general scope of antivirus software. Alone, a single security technology is not sufficient to defend against these blended threats, as was demonstrated by the Nimda and Code Red attacks.

CONSTRUCTING A CURE

The complex, destructive nature of these threats illustrates how the primitive strategy of “one threat, one cure” approach is out of date. Consistent, widespread security solutions that provide several layers of defense are required for protection against blended threats.

Working in combination, the following layers of protection will help ensure the confidentiality and security of the company’s data:

1) **Antivirus software and content security solutions.** The most important step in combating malicious threats is to install antivirus software. This software will scan for and detect viruses, as well as repair any damage resulting from a virus. Antivirus software and content security solutions are generally used to identify and remove threats.

2) **Firewall software.** An effective firewall is an organization’s first line of defense against hackers. Firewalls establish guarded gateways that are designed to keep the information on the inside safe from anyone on the outside. They inspect incoming information and block those that do not meet criteria specified by an administrator, such as blocking access at particular ports or based on the length of packets. Firewall software can help to fight against inbound and outbound attacks by blocking threats from entering an organization’s network.

3) **Content filtering tools.** Content filtering tools applied at Internet gateways can also help the enterprise to proactively identify potential threats. These filtering tools stop harmful viruses and malicious code at the network gateways before they even have a chance to penetrate a user’s computer. They are provided through establishing content policies and corresponding rules including subject line, content and spam rules.

4) **Vulnerability assessment tools.** Vulnerability assessment tools help ensure that patches are applied, unneeded services are removed and passwords are strong, according to best practices. Vulnerability management solutions allow IT administrators and IT security managers to create, manage and install customized security policies across their networks.

5) **Intrusion detection systems.** Intrusion detection systems offer significant detection and prevention capabilities against attacks. These systems are used to monitor the network and hosts for improper activity and assist in forensic analysis. They are aimed at finding the network’s weak points.

Security technologies need to be instituted on all levels and for all users, including remote users. In-Stat predicts there will be 17.6 million telecommuting workers in the U.S. by 2005. With this figure in mind, it is crucial that remote machines have at a minimum installed antivirus software and personal firewalls. Telecommuters open up another potential window for corporate network infection, and if these machines are unprotected on the Internet, all of their critical business information could be subject to attack. Also, these tools and systems need to be continuously updated in order to protect against the most recent and complex threats.

INDIVIDUAL VS. INTEGRATION

In developing this layered security solution, there will be a number of individual security products from different vendors that need to be purchased, installed, deployed, managed and updated separately. With this compound approach, IT managers are faced with the issues of interoperability and consistency among their extensive security layers. There are also considerable staffing and budgetary issues to consider. Selecting, installing and maintaining each of these products is a lot of work and can be quite costly. Further, monitoring the security world to determine what new products one needs is also time-consuming. Protection is not all-encompassing because of these issues, which often allows threats to slip through the cracks, therefore compromising security.

Integrated security solutions emerged out of the need to manage and combine all of these security functionalities into one appliance. Integrated security provides a “total” solution and improves the overall security in a way not possible by simply implementing individual products from many different vendors. By combining multiple security functions, such as antivirus, content filtering, firewall, vulnerability management and intrusion detection, integrated security can more effectively and reliably protect against a variety of threats at each and every tier.

Also, technology alone does not address all security issues. Don’t let oversight and negligence leave a system vulnerable to intruders and viruses. Make sure to implement and execute various security standards internally. Establishing firm policies and procedures can help plug any undetected holes in a system. Removing unneeded services, implementing strong passwords, keeping patches up to date, data forensics and other critical strategies can help enhance your overall protection. By increasing awareness and understanding of the enterprise’s systems, IT administrators will be one step ahead of any possible electronic attacks.

The combined defense of advanced security technology and effective end-user policies will provide the strongest weapon against the spread of malicious blended threats.

COMBATING THE UNKNOWN

Viruses have become significantly more complex and are now able to spread their destruction faster and farther than ever before. As virus threats quickly evolve and increase in complexity, managing these threats becomes a great challenge. As defending against simultaneous, multiple Internet threats becomes imperative to enterprise security, IT managers will likely be looking to software vendors to provide a total security solution and ongoing support. The latest blended threats are propagating at an ever-increasing rate, forcing security companies to reevaluate their strategies and technologies. Virus solution providers are refining technologies and offering alert systems, such as the emerging class of early warning solutions, to help enterprises and individuals better manage the challenge.

These comprehensive alert systems help increase awareness of potential attacks by delivering customized early warnings of any prospective threats worldwide. Early warning solutions include customized threat analysis tools as well, in order to predetermine possibilities of attacks. These solutions also provide preparatory countermeasures for any approaching threats, therefore preventing attacks before they occur.

While security vendors are doing their part in creating and distributing the most advanced and innovative solutions of the times, like early warning systems, IT administrators need
to do their part as well. By taking a more comprehensive and adaptable approach to security, organizations can quickly and proactively address existing as well as emerging threats from malicious threats.

There’s no doubt that virus authors will continue to design new viruses, using new technologies, creating new problems. Who knows what they’ll think of next? It is anticipated that blended threats will occur more regularly and will grow in complexity in the future. As more money is invested into IT departments and staffing, enterprises have much more to lose financially should they be hit by a major attack. However, integrated security solutions are certainly a step in the right direction towards the prevention of such loss.

Organizations can now benefit from integrated security in a variety of ways, including improved efficiency of security functions, minimized business impact of attacks and an improved overall security posture. In fact, companies that adopt an integrated security strategy today will be in the best position to take advantage of the next stage of integrated security, whereby all network tiers will be integrated and centrally managed. Through this enterprise-wide integration of security, administrator resources will be optimized, as installation, reporting and updates will be possible from a single console. This management capability will further improve protection, while reducing the administrative, support and ownership costs typically associated with enterprise security.

NaSPA member Cosmo Battinelli is vice president of technical support for Symantec. Battinelli brings 25 years of experience in IT development and product and customer support. He can be reached at cosmo_battinelli@symantec.com.