SecurityManagement®
March 2004

COMPUTER SECURITY

As traditional antivirus protection has been outpaced by new types of malicious code, companies are challenged to find more effective solutions.

Defenses Morph as Viruses Mutate

By Peter Piazza

If current antivirus products were truly effective, businesses would be winning the war on computer viruses. A 2003 survey conducted by the FBI and the Computer Security Institute found that no fewer than 99 percent of the 530 respondents were using antivirus solutions. Yet the same survey indicated that 82 percent of organizations had nevertheless been infected by a virus (the term "virus" includes other malicious code such as worms). The reason for this incongruity, computer security experts say, is that traditional antivirus protection, which targets specific attack signatures, has been hindered by several weaknesses. Consequently, it has been outpaced by new types of malicious code.

The next few years will see vendors trying to iron out the kinks in existing intrusion prevention and detection systems.

For example, antivirus programs require constant and regular updating (even then, they are typically only effective against known threats), and any delay in this process leaves networks vulnerable. But perhaps the greatest challenge to antivirus program developers is that malicious code writers are becoming more savvy.

The problem. Malicious code writers understand the methodologies in which antivirus is deployed, "and so they're writing code to get around antivirus software," says John Frazzini, vice president of intelligence operations at iDefense, a Reston, Virginia-based security intelligence company. This includes "hybrid" threats that have both virus and worm characteristics, according to Mark Loveless, a senior security analyst with BindView, a Houston, Texas, company that makes security software.

"What's happening now is there is more of a trend for viruses to take on worm characteristics and also use multiple attack networks," explains Loveless. Rather than simply spreading via infected e-mail attachments, which traditional antivirus solutions can block (assuming the signatures are up to date), malicious code can now directly exploit system flaws, such as servers that have not had a particular patch installed.

And while hybrid threats are not brand new, they are becoming more sophisticated, says Rob Clyde, chief technical officer with antivirus company Symantec, based in Cupertino, California. "We're entering an interesting era of these combination attacks that are blended both deliberately (such as Blaster or Nimda) or accidentally," he says. In some cases, Clyde adds, the hybrids have mutated even beyond the intentions of their creators. Symantec's honeypot (a decoy system set up to trap malicious code that can then be examined) has even trapped

It used to be that if an organization had strong protection around its perimeter, most threats could be blocked. That's changed.

worms that have been infected by viruses, he says. "The worm actually becomes a carrier for this virus coming into the network, which then turns around and tries to infect additional programs on the system and does more damage than the original worm ever intended," he explains.

According to Frazzini, the problem of keeping up with savvy code writers is compounded by another issue: The time needed to create, distribute, and install virus signatures when a new virus is discovered makes the update process cumbersome and reactive.

Porous perimeters. Further complicating the fight against malicious code is that perimeters are more porous than in the past. It used to be that if an organization had suitably strong protection around its perimeter, most threats could be blocked. But that's changed, experts say. For example, despite the widespread use of firewalls (98 percent of respondents to the computer security institute survey had firewalls in place), virus and worm attacks can and do still succeed.

Perimeter security is "like having a letter box opening on a nicely protected front door," because all firewalls are designed to let approved traffic through, says Peter Glock, head of the security product line for the U.K.-based managed security services provider and Internet service provider Equant. Application-level attacks, such as buffer overflows or cross-site scripting, defeat perimeter protection by taking advantage of these openings. "By doing something that looks like legitimate activity, with an information resource that an enterprise has opened up, I can actually do something malicious," he says.

Loveless points to the practice of allowing large customers and other trusted partners access to a corporate intranet as another danger. Similarly, companies now allow remote workers using laptops to go out and connect to a lot of different networks, notes Glock. These users "get infected by whatever means (it might be a virus or a Trojan or a worm) and then bring it back into the nice secure, safe environment in the office, and pass that infection around inside all the defenses that someone has put into place."

Solutions. The solution lies both in technology and in management of the systems. Of course, keeping software updated and installing patches is essential. The more that this process can be automated or at least automatically checked, the better. Equant, for example, has tried to enforce good antivirus solutions by "putting policy engines on everyone's PC," Glock says. (A policy engine is a software program used to enforce company policies, allowing or disallowing user requests based on any number of criteria.) "The policy engine doesn't let one connect to the network unless the user has run a virus scan recently and is using an up-to-date virus scanner with up-to-date pattern files," says Glock.

Signature-based antivirus software. Given its shortcomings, will signature-based antivirus software continue to play a role in the fight against malicious code? Experts interviewed for this article say yes, but that role is "becoming smaller in terms of relevance," explains James Hurley, vice president and managing director of information security with IT market analysts Aberdeen Group. He calls signature-based technology an "annuity business for the suppliers, because they just keep pumping out new pattern files and you have to sign up for it." But, he adds, if there is a better way to prevent problems in the first place, it raises the question of whether that annuity business can survive. It probably can, he says, "but my bet is that suppliers of antivirus are a little worried about that," and there is no shortage of technology that promises an alternative solution.

Virus and Antivirus: The Basics

To understand the danger of malicious code and the weaknesses of current antivirus solutions, it's important to first review how malicious code works and how traditional antivirus solutions protect against such code. Viruses are pieces of code that can only infect a computer with the help (typically unintentional) of a user. They piggyback on programs, and each time that program is run, the virus can infect other files. A virus cannot infect another computer by itself; it needs the help of a human who might attach an infected file and send it to a colleague. Once that person opens the infected file, the virus spreads.

Worms take this concept to a new level. First, they need no assistance to spread. Some worms include engines that allow them to send—without assistance—an infected e-mail to every address located in an address book, for example. But they don't rely solely on e-mail to infect new machines. Worms can take advantage of flaws in software code that allow them to infect other computers that have the same flaw, and so they can very quickly compromise an entire network.

Viruses and worms can carry a payload ranging from the relatively benign (a message boasting of the infection) to the devastating (deleting files or targeting another network in a denial of service attack). But it's not only the payloads that give malicious code the opportunity to wreak havoc across the Internet. Some are so proficient at seeking out new victims that they shut down a network simply by using all its bandwidth.

Most antivirus solutions have relied on recognizing the pattern of known malicious code to block viruses at the point where they typically enter the network: the e-mail gateway. Antivirus companies regularly update these "signatures" to reflect the newest versions and variants of e-mail-borne viruses. If administrators keep antivirus signatures up to date, most or all of the known viruses will be blocked wherever the antivirus product is installed.

Another, less common type of antivirus solution uses heuristics—that is, it makes decisions on whether a virus is present based on the behavior of the code. Although heuristic-based antivirus was once considered to hold great promise, this technology has never overcome its limitations. For example, excessive reliance on heuristics "leads to some unwanted side effects, such as excessive false positives or negatives," says Chris Belthoff, senior security analyst with U.K.-based antivirus company Sophos. Although Sophos uses heuristics "judiciously," Belthoff says, he believes that signature-based antivirus remains the major method.

Combining technologies. It seems clear that antivirus vendors are indeed worried. Recognizing their limitations, many companies that develop signature-based antivirus programs have begun to invest in ways to provide broader solutions. In August 2002, for example, Symantec spent more than $200 million acquiring Recourse Technologies, which makes intrusion detection technology, and SecurityFocus, which collects intelligence on new bugs, vulnerabilities, and malicious code. At press time, another Symantec deal to acquire a patch-management solution was also in the works. Other companies have followed suit, and since 2002 this industry trend toward the integration of multiple functions has evolved from concept to implementation of new products.

Symantec's Clyde explains that Recourse created "true second-generation intrusion detection technology that was heavily based on protocol anomaly detection and statistical flow analysis," and also incorporated signatures to identify known attacks. (Like antivirus software, intrusion detection products have depended heavily on signatures that allow known threats to be identified. Anomaly detection and flow analysis look instead for deviations in patterns of behavior or traffic.)

The purchase of SecurityFocus was an inspired move, says iDefense's Frazzini. SecurityFocus is a vendor-neutral Web site that includes the well-respected BugTraq, which bills itself as "a high volume, full disclosure mailing list for the detailed discussion and announcement of computer security vulnerabilities." A database of current vulnerabilities is also part of the site.

The database is freely available, but those who do not subscribe to Symantec's paid service don't get new postings until 48 hours after they are first posted; given the rapidity in which new vulnerabilities are turned into exploits, two days is a long time.

Frazzini notes that intelligence gathered through the site now powers the company's intrusion prevention and detection devices and antivirus solutions, and it gives the company the chance to create protection against threats before they arise.

Taking the same tack, antivirus vendor Network Associates acquired IntruVert, which creates network intrusion prevention products, and Entercept, maker of host-based intrusion prevention. Trend Micro announced a partnership with digital security company eEye to provide a virus vulnerability assessment service. (eEye also performs security research including virus analyses and has discovered many major software vulnerabilities, thus supplying an intelligence component to the mix).

Finnish antivirus company F-Secure has taken a slightly different road to the same destination; rather than acquire product, it has developed its own integrated suite. The company released its Anti-Virus Client Security product in September 2003, which includes a firewall with intrusion prevention and automated virus-definition updates.

But it's not only traditional antivirus companies that have combined in recent months to find new ways to fight malicious code. In December of last year, network firewall and virtual private network (VPN) vendor Check Point acquired Zone Labs, which makes desktop firewalls; the acquisition recognizes that network perimeters have weaknesses and that defense in depth—many layers of security at different parts of the network—is needed for adequate protection. Even Cisco, best known for making the bulk of the Internet's routers and switches, has taken steps toward integrating protection products into its own products. In 2003 it acquired Okena, a maker of host-based intrusion detection and other security software.

In addition, last year Cisco launched the Network Admission Control (NAC) program in conjunction with Symantec, Network Associates, and Trend Micro. The antivirus companies have licensed a component of NAC, a small software agent installed on computers and servers that tells Cisco routers (and, in future releases, other products such as switches and wireless access points) whether the antivirus signatures of those computers are current.

NAC also collects data from other security devices such as firewalls, which makes it possible for the Cisco hardware to enforce access privileges. A computer that doesn't match a company's policy (for example, it does not have current patches installed or its antivirus software is not up to date) can be blocked, quarantined, or even sent for remediation. This feature helps maintain consistent security policies for computers connecting to the protected network.

From the end user's perspective, the merging of these technologies is intended to make system management easier. Whether that will be the result remains to be seen. "Half the battle is to get every bit of the information from all of these products into the same console for enterprise management," says BindView's Loveless. Once all the data is consolidated, the ability to correlate events may indicate worm activity. But "no one's there yet, regardless of what their marketing departments may claim," he says, although "they're heading that way."

Belthoff of Sophos agrees. "There's still a lot of progress that needs to be made in those areas with respect to having a truly effective tool," he says.

Integrated systems remain a work in progress in part because the individual pieces are still being developed and refined. For example, Nazario believes that the next few years will see vendors trying to iron out the kinks in existing intrusion prevention and detection systems, in part stimulated by a recent request for proposals from the Defense Advance Research Projects Agency (DARPA) for new methods of "dynamic quarantines" for countering worms.

DARPA's expectations are high: milestones for the second phase of the program demand that worms released on a testbed be contained to one percent of vulnerable machines; the false positive rate is limited to one per day; and recovery of infected systems must be achievable in six minutes or less. Nazario says he doesn't know of any existing averages for such products, particularly given the huge number of variables (from the size of a network to the actions necessary to recover the network). He notes that there are products that already meet some of these milestones under certain conditions, but he adds that it may not be possible to achieve all of them.

Despite the many difficulties, there is progress being made. "It's exciting and heartening that people are looking at real solutions to these problems," Nazario says. "If you look at broader descriptions of the problems and try to address them at that level, then we're moving closer to at least being on par with, if not a step ahead of, threats." ■

Peter Piazza is assistant editor with Security Management.