[By Dennis Fowler]

Attack of the KILLER VIRUS!

Though more than 600 million people worldwide use the Internet, it takes only one virus writer to make just about all of us miserable. Like a single stray neutron in a critical mass of plutonium, a lone virus can trigger a chain reaction that spews thousands of copies from desktop to desktop. Last summer's aptly named SoBig virus was an all-too-real example of this danger. "At [SoBig.F's] peak, one out of 17 e-mails that we were processing was a copy of the…virus," says Josh White of U.S.-based e-mail security group MessageLabs. "Certainly we haven't seen numbers

Illustration by Dynamic Duo Studio.com

like this before." At that time AOL scanned 40.5 million e-mails and found SoBig.F in half of them. In fact, SoBig accounted for 98 percent of all viruses then circulating—all this from a single virus-writing miscreant. How can we possibly hope to stop the inevitable legions of similarly determined troublemakers? Better get used to it: There are no easy solutions to the virus problem.

Blaming the Victim

What, do you suppose, is the percentage of users who will open and run an e-mail attachment from a total stranger? Five percent? Ten percent? Maybe more: In an article in the September 12, 2003 issue of *The New York Times*, a study is cited where a test virus was e-mailed anonymously to 13 members of a bank's computer security team. "Five members of the I.T.-security-savvy team in the financial sector executed an in-your-face [virus]," reported Roelof Temmingh, technical director at South Africa-based SensePost Information Security, at a July security conference in Las Vegas. That's over 38 percent. One can only imagine the percentage of less-sophisticated users who would have acted exactly the same way.

The temptation is to blame careless users for unthinkingly launching these infections, blame them for not keeping their systems patched, protected with anti-virus software, for not implementing firewalls. "In all fairness, users aren't so much 'careless' as overwhelmed by a world not their making," says Karen G. Schneider, director of the Web portal, Librarians' Index to the Internet (http://lii.org/). "The sales pitch has been 'technology will change your life.' The part we all left out is 'yes, but not necessarily for the better.' So they go online to send e-mail to their kids, buy dresses from Sears, and otherwise participate in our 'paperless society'…and the next thing they know, they're grappling with spam, viruses, updates, pop-ups, opt-outs, and buckets of questionable information, plus the message that anytime an alligator bites them in the butt, it's because they are 'careless.'"

"Users open PIF attachments because they're attached—why would they know enough about computers to know which files to open and which not to open?" asks Michael "Mac" McCarthy, VP Editorial and Portals, DevX Division/Jupiter Media Inc. "A technology this widely used can't reasonably expect that level of expertise from its users; it's simply impractical." Besides, with multi-vector viruses like Blaster, which spread both via e-mail and through an unguarded port 135, the average home user can be infected even if no e-mail is received, no attachment is activated. In any case, the average user is unlikely to take the pro-active step of keeping the system patched, anti-virus software up-to-date. Most don't know what a firewall is, let alone how to implement it.

Pros to the Rescue?

Even if we could depend on the average user, a heavy burden rests on IT departments and ISPs to make sure their patches are up to date, their filters enabled. That is easier said than done.

"[Administrators] don't apply patches regularly," McCarthy points out, "because the patches themselves are buggy and crippling just often enough for it to be the conventional wisdom…to let patches cool off for a few months before applying them. Now [administrators are] happy to discover they're screwed no matter what they do—install all patches right away and risk screwing up the system…or wait and only install patches that have proven themselves. And when hackers jump in…you get abuse from your users—and the press."

Mandatory patches have been emerging from Microsoft at an average of more than once a week. Clearly we can't depend on

users or administrators. Who's left?

Can Programmers Be Held Liable for Software Breaches?

The end-user license we agree to when we open a software package almost always says that there is "NO LIABILITY FOR CONSEQUENTIAL DAMAGES," or words to that effect. As the flaws and holes in Windows mount, so does a cry to hold Microsoft accountable. That clause now faces a legal challenge, thanks to a suit filed in October in Los Angeles Superior Court. Claiming Microsoft's "eclipsing dominance in desktop software has created a global security risk," a suit was filed on behalf of a mother of two from Los Angeles whose identity was stolen thanks to a hacker invading her system.

"We represent an individual plaintiff who is also seeking to be a class representative on behalf of all U.S. purchasers of Microsoft operating system software," said attorney Dana Taschner, the Newport Beach, California, who filed the suit.

At the time of this writing Microsoft is studying the action. They hope to quash the class action certification, which would effectively neutralize the suit. The company blames the problems on the hackers who write the worms and hack the systems, not on their own failings.

If a locksmith knowingly sells flawed locks, can he be held liable for the burglaries that result?

If the class action request is accepted, Microsoft may find itself facing monumental liability claims. Bruce Schneier, CTO of Counterpane Security and a noted computer security expert, hopes they do. "Maybe then Microsoft will finally get the message and secure their software," he says. But can they?

In Fairness to Microsoft

Totally securing an operating system any operating system—but particularly Microsoft Windows—is incredibly challenging.

In "CyberInsecurity: The Cost of Monopoly," a report written by a half dozen independent security experts (Bruce Schneier included) and published by the Computer & Communications Industry Association (CCIA, www.ccianet.org/index.php3), the authors note that complexity drives the creation of security flaws and that "experts often describe software complexity as proportional to the square of code volume."

The report says Windows NT code volume increased 35 percent per year, that complexity increased 80 percent per year. Internet Explorer code volume increased 220 percent per year, increasing complexity 380 percent per year.

Another source of Windows' vulnerabil-

TOTALLY securing an operating system—any operating system, but particularly Microsoft Windows—is incredibly challenging.

ity has been Microsoft's focus on ease of use. There's always a tradeoff here: As anyone who has taken a flight on a commercial airline in the last two years can attest, the greater the security, the greater the inconvenience to the traveler. And inconvenience is not exactly what the public seeks in an operating system.

Also, as Microsoft integrated their components more tightly with each other and with the basic operating system, in an effort—so they said—to enhance compatibility (and, again, make the product easier to use), vulnerabilities multiplied further. An opportunisitic worm entering the system via Instant Messenger, for example, might access Outlook for addresses to which it can mail itself, or it might raid databases containing credit card information and transmit that data back to an identity thief.

Now virtually any effort to close vulnerabilities may make things worse, and will unavoidably make the system more challenging to use, alienating customers. Already, if a user implements the strictest security in Internet Explorer, he or she will be so pummeled by warnings as to make surfing the Web unbearable. Blocking pop-up windows, Java script or Active X controls makes some Web sites virtually inaccessible.

In short, no matter what they say, Microsoft is in an untenable position. The company's operating system is so complex, that the odds of fixing every potential vulnerability are extremely low. Chances are good that the patches will either break something or introduce an unexpected vulnerability, and ease of use is bound to suffer. Simply adding a default firewall presents the average user with yet another component to configure, or, more likely, disable, because they don't understand what it is or how to use it.

THERE is security, of a sort, in a diversified computing environment. With fewer targets single-platform viruses find it harder to spread.

Even getting users to implement patches is a challenge. Automatically upgrading a user's system via download seems a better idea, though AutoUpdate (which made its debut in Windows ME in 1999) is hardly something new. But what if the "fix" is itself flawed, damaging the user's system, which already happens with conventionally distributed patches?

In addition, the sheer volume of the accumulated patches for Windows XP makes downloading them impractical for those limited to dial-up speeds. The Japanese division of Microsoft is handing out free CDs with vital patches, but there's no sign that U.S. users are going to receive the same courtesy. Even if they do, how many users are going to avail themselves of the offer?

The Antivirus Arms Race

Antivirus vendors are continually playing

catch-up. Not unlike a biological immune system battling microbes, the infection comes first, then the antibodies.

Unfortunately, the antivirus forces are always going to be one step behind. They can't start churning out the cure before the infection is detected. The speed demonstrated by nasties like SoBig and Slammer, which infected virtually every vulnerable machine on the Internet within 10 minutes of its appearance, means that the infection can get a monstrous head start before countermeasures can be implemented.

We are running out of options. But what's left?

Is There Security in Diversity?

There are those who say that only Windows is vulnerable to viruses and only Windows viruses are written.

They're wrong. No operating system is invulnerable to viruses. Back in the days before Windows there were DOS viruses. Early Macintosh viruses were actually more contagious than DOS viruses because they were buried in the Macintosh file system's resource fork, making them easily transmissible by download.

Some loyalists claim Linux is virus proof. Windows loyalists counter with "No one bothers to write viruses for Linux because it has such a small market share."

They're both wrong. There are Linux viruses, but so far they have been relatively harmless. There is Linux antivirus software, in itself an admission that Linux viruses are for real.

It is true that the vast majority of viruses are written for Windows. Dr. Nic Peeling and Dr. Julian Satchell, in their report "Analysis of the Impact of Open Source Software" (www.govtalk.gov.uk/documents/QinetiQ_OSS_rep.pdf) note that "There are about 60,000 viruses known for Windows, 40 or so for the Macintosh, about five for commercial Unix versions and perhaps 40 for Linux."

The report gives two reasons for Windows' greater attraction for virus writers compared to Linux. The first is its popularity. Not only does that make it a more tempting target, but "For a virus to spread, it has to transmit itself to other susceptible computers; on average, each infection has to cause at least one more. The ubiquity of Windows machines makes it easier for this threshold to be reached."

Secondly, they go on, "Windows has had a number of design choices over the years that have allowed the execution of untrusted code, and this has made it a very easy target."

Linux, on the other hand, isn't such a push-over. In an article posted last June in *The Register*, SecurityFocus's Scott Granneman notes that "a Linux user would have to read the email, save the attachment, give the attachment executable permissions [which requires 'root' privileges], and then run the executable."

Of course, this very complexity is one of the reasons Linux has been slow to gain market share.

Now, just to give us more to worry about, a new complex cross-platform Windows/Linux virus has appeared. Not the first, but the most challenging of the breed so far. Simile/Etap was discovered late last May and is described as a "very complex virus that uses entry-point obscuring, metamorphism, and polymorphic decryption," making it very hard to detect.

Simile/Etap infects Portable Executable and 32-bit Executable and Linking Format files on both Linux and Windows systems. It contains no destructive payload, but displays messages on September 17th and March 17th. The infection threat in the wild is said to be low. For a Linux user to be victimized he'd have to be logged in as root and run suspicious e-mail attachments.

However, Marius van Oers, an analyst

at McAfee, warns that "…there is no technical reason why Unix shell script malware cannot be successful in the future—it is a matter of proper coding combined with suitable or less secure environments."

So Linux users need to worry, too.

However, there is security, of a sort, in a more diversified computing environment. With fewer targets, single-platform viruses find it harder to spread. A mixed Windows/Linux network is much less likely to be brought down completely by a Windows virus. Since cross platform viruses are harder to write there are fewer "Typhoid Marys" to worry about.

The CCIA report cites this as a reason for breaking Microsoft's grip on the market.

So Deal with It

So we are left with one of those seemingly insoluble issues that dot today's digital landscape, along with spam and preserving intellectual property rights. There are no viable solutions to the viral epidemic—at least not yet.

When the first Model T came out only a mechanic could embark on a trip of more than 20 miles with any certainty of reaching his destination. Breakdowns and flat tires were as inevitable as computer viruses are today. We are still in the early Model T era of the Internet today. If we are to move forward, software developers must learn to build operating systems that are both easy to use and 99.99 percent reliable—just the way most cars emerge from the factory today.

And while we're at it, how about warranties that mean something? It's amazing how automobiles improved when the five-year, 50,000-mile warranty became common. Computer users should be notified of a recall, and dealers should offer trained "mechanics" who will fix critical flaws under warranty, with free parts and labor. Maybe if Microsoft had to bear the full cost of fixing these problems they'd never let them out the door in the first place. And if Linux wants to survive it will have to meet the same standards of service, or go the way of the Nash Rambler.

Users need firewalls and antivirus software as easy to implement as the lock on their steering column. Administrators need the equivalent of a good automated pothole filler, while authorities need the digital equivalent of radar guns and pursuit-cars geared to catch the moonshiners and street racers wreaking havoc on the information superhighway—which, by the way, could use better paving and a lane banning trucks carrying junk mail.

At this point, our best chance of avoiding a truly crippling epidemic is to get the jump on new infections as they come along. It's reasonable to assume that a new virus, like the beta version of any computer code, will be buggy. The engineers at AT&T claim to be working on an early warning system to alert the company's customers to new threats based on just that premise. They hope to issue warnings as soon as they see the first inklings that someone's trying to unleash a new virus.

"We see the fizzled versions of stuff in advance," says Ed Amoroso, chief information security officer at AT&T. "We're trying to change the nature of our relationship with customers so when we see...indicators of something that fizzled, we tell everybody."

Perhaps anti-virus vendors really can learn to get antidotes out there before finished viruses "ship." Then administrators can circle the wagons, implementing remedies before real assaults are launched. This is a glimmer of hope for a problem that we should expect to be dealing with for many years to come. ~

Dennis Fowler *has been a freelance writer for over 30 years. For the last decade he has been following the computer industry, specializing in online issues and the Internet.*