



If you're among the lucky group of small office/home office users who have "broadband" Internet service (usually defined as a connection that can carry at least 384 kilobits per second from the Internet to you), consider yourself fortunate. You enjoy a level of access that, only a few years ago, was only available to large corporations at a cost of thousands of dollars per month.

Rough Water

But a high-speed onramp to the information highway does not necessarily mean smooth sailing for Web surfers. Some of the problems you'll encounter will be mere annoyances. You may discover that performance is more uneven than before because, while your Net connection is now fast, the connections of many of the websites you access are still often congested or slow enough to cut your browsing speed. But the most serious threat--one that ISPs, telephone companies, and cable companies rarely acknowledge--is that of security breaches.

High-speed connections also allow unwanted intruders to get in and out faster and try more methods of attack. The high-speed connection itself makes you a more tempting target. Even if the attacker isn't human--that is, if it's a Trojan horse or worm--it can do far more damage to you and others when it exploits a broadband connection to spread itself.

"What would an intruder hope to gain by breaking into your home or small office computer system?"

The pages that follow explain the risks and tell you what you can do to protect yourself, your family, your bank account, and even your reputation from the more frequent and potent security threats encountered in high speed connections to the Net.

Why Me?

If you're a typical broadband user, your reaction to the statements above might well be, "Why me? There's nothing much of value on my machine--just the browser I use for the Web, plus my recipes, some letters, and a few household documents. Why would a hacker care about breaking into my system?"

Good questions. What would an intruder hope to gain by breaking into your home or small office computer system?

Chances are, they're after one or more of the following things:

- **Your bandwidth.** With 384 kilobits to more than a megabit per second of bandwidth, your DSL or cable modem is capable of sending and receiving a lot of data very quickly. While it's unlikely that you give your broadband connection a 24x7 workout, hackers can find lots of things to do with it. For example, your system, together with others that have also been co-opted, can be used to unleash huge barrages of data on other computers on the Internet, rendering them useless. (This is called a distributed denial of service, or DDoS, attack.)

Hackers can also use a compromised machine as a jumping-off point for difficult-to-trace attacks on other machines. This is especially likely to occur if you're using certain vulnerable software, such as older versions of the Wingate connection-sharing software. This software makes the attack appear to come from your machine when, in fact, it's coming from somewhere else. However you're still liable for the actions of your machines whether you like it or not.

- **Your computing resources.** If hackers take over your system, they can turn it into an Internet server that does their bidding. They can use it as an illicit "meeting place" by setting it up as an IRC (Internet relay chat) server, or use your hard disk as a repository for illegally copied software ("warez"), movies or music. We've discovered systems--most often running Microsoft Windows that have been used to hold gigabytes of illegally copied music, video, and expensive software such as Microsoft Office. If the copyright sleuths that prowl the Internet identify your machine as the source of such materials, your ISP may blame you for the copyright infringement and attempt to cut off your broadband service.

- **Your personal data, your identity, your reputation, and/or the contents of your bank account.** Do you prepare your taxes on your computer? Pay your bills using a service such as CheckFree or Paypal? Have any files at all containing your credit card numbers, Social Security number, or other identifying information? If so, you're a potential target for identity theft, an increasingly common crime in which a thief gathers sufficient information to impersonate you.

The havoc that an identity thief can wreak in your life is almost unlimited. He or she can change the addresses on bank, credit, and brokerage accounts, diverting statements so you won't notice that something's amiss. He can then sign up for credit in your name, sell your investments and pocket the proceeds, and drain your bank accounts. If you have a debit card, the thief can wipe out the account to which it is attached in a single transaction.

The *Fair Credit Billing Act* was passed during a very pro-consumer period of US history to protect US citizens from fraudulent charges on credit cards. But debit cards did not exist at the time and, therefore, were not covered. If a thief is operating from afar, especially from a foreign country, you'll likely have no recourse. If a criminal manufactures false identification with your name on it, you could even find yourself accused of crimes, with warrants issued for your arrest when you have done nothing wrong. Other entities may also collect data about your Web browsing habits or computer usage without your consent--and then offer it for sale to all and sundry.

While snooping techniques affect all Internet users regardless of the way they connect, a high speed connection masks their presence by preventing them from taxing your bandwidth.

In the sections that follow, you'll learn about some of the most serious Internet threats--and the ways in which a broadband connection can amplify their dangers.

Opening Windows On File-Sharing Abuse

One of the most common ways hackers attack broadband users is to exploit the built-in file sharing features of Microsoft's Windows operating system. Windows machines come equipped, out of the box, to share files with other machines on the same network--a feature called "peer to peer file sharing." While users who turn this feature on may think that they're sharing files only with other computers in the same house, it's unfortunately all too common to find that they're

really being shared with the entire neighborhood--or the entire Internet. "Worms"--described in more detail below--can also enter via Windows' file sharing features, infecting and possibly disabling your computer.

IE, OE, et al...

Internet Explorer and Outlook Express as well as the full Outlook e-mail client and personal information manager, are rife with security holes, and new ones seem to surface daily. Browsing with many versions of Internet Explorer (especially in their default configurations), or checking your mail with a Microsoft e-mail client, could allow your system to be infected so quickly--thanks to your high-speed connection--that you have no chance to react before your machine is harvested for data or damaged beyond repair. At this writing, several widely circulated worms, such as Magistr/32 or Sasser, are capable of destroying your machine's BIOS (Basic Input/Output System), rendering your machine unable to boot.

Another common point of entry for hackers targeting Windows systems is a utility called Wingate, which many broadband subscribers use to share a high speed Internet connection among several machines in their homes or offices. While newer versions of the utility are secure, older ones--which are still out there and are often pirated--allow a hacker to "tunnel" through your machine on the way to the rest of the Internet, hiding his or her identity.

Pirates' Lair

One increasingly common exploit is not limited exclusively to Windows machines. It occurs when hackers locate a machine that's been set up as an anonymous FTP server, a file repository that anyone can access. If your machine is configured to allow anyone to upload and download files--or if a hacker breaks in and sets it up that way--you may soon find that it has become a repository for pirated software, music, and even video.

"No person shall circumvent a technological protection measure that effectively controls access to a work protected under this title..."

Digital Millennium Copyright Act

A newly passed Federal law, the *Digital Millennium Copyright Act*, compels ISPs who are notified of this form of abuse to stop it or face serious penalties. So, by the time you discover that your system is being used in this way, your broadband access may be cut off. It's your broadband connection that makes your machine an appealing target for this form of abuse because large uploads and downloads aren't practical without lots of bandwidth.

Many versions of Windows are also subject to other security exploits ranging from the "Ping of Death" (which merely causes the machine to stop working) to "Back Orifice" (a program that lets a hacker do whatever he or she wants with your machine via remote control).

Just Say No

The ideal solution to Windows' security problems might be to scuttle the operating environment altogether and install UNIX. Unfortunately, for most people, this is not a viable option. Many machines were designed only to run the insecure, but ubiquitous, Windows. And most of us have no inclination to master other more sophisticated--but also more obscure--operating systems.

Because Windows is so vulnerable, it's vitally important for those who run it to take the security measures outlined in the "Self Defense" portion of this article.

Malware, or malicious software, is a threat to the integrity of any computer. But the risk is especially great when that computer has a high speed network connection.

In the early days of computing when computers were not networked, viruses were actually quite difficult to spread. The primary vector for malware was floppy disks. One often had to mistakenly boot the machine with an infected disk in a particular drive to become infected. A virus that spread in this way was called a boot sector virus.

Next came the age of the computer bulletin board system (BBS) and proprietary online services such as CompuServe, Prodigy, Delphi, and QuantumLink (which later evolved into AOL). During this period, many computer users downloaded files at a relatively slow 300 to 2400 bits per second. Trojan horses--programs that look like legitimate programs but are really destructive--began to propagate, mostly as pranks. File-infesting viruses, which incorporate themselves into program files on your machine, also began to spread.

Nonetheless, thanks to vigilance and careful checking on the part of "sysops" (system operators), malware remained an occasional annoyance rather than a serious threat. It was not until the Internet blossomed from an experimental academic playground into a global commons that malware became a serious hazard.

The Worm Turns

The turning point, according to many, came in 1988, when Robert Tappan Morris Jr. set loose a worm. A worm is malware which, unlike a virus or Trojan horse, does not

require action by the computer's user to spread. Using the Internet's high speed connections between colleges, government installations, and research institutions, the worm quickly broke into--and took down--a substantial number of the machines that were then on the Net.

One would think that the Morris worm would have been a wake-up call to operating system designers and system vendors worldwide. But most of the world still was not networked. Vendors ignored the ease with which this relatively simple malware virtually took over the Net and they did not build good security into their products.

"At approximately 5 PM on November 2, 1988 the 'Morris Worm' was started at the MIT AI laboratory in Cambridge, Massachusetts. It quickly spread to Cornell, Stanford, and then on to other sites. By the next morning, almost the entire Internet was infected. "

Source: worm.net

Today's Internet connections, which are tens or hundreds of times faster than those available in the days of the Morris worm, allow malicious agents to mount attacks far more potent than before. A 512 Mbps DSL connection could, in theory, allow an attacker to try more than 5 million 10-character passwords per second while trying to break into a machine.

An attacking program can identify your machine's operating system, down to the specific version, in an instant using a technique known as TCP/IP stack profiling. It can then scan for potential vulnerabilities by doing a port scan. Finally, it can attempt multiple, simultaneous attacks--all customized to have the greatest chance of success. And the entire scanning and break-in procedure can be performed automatically on dozens of potential victims at once. The Ramen and Adore worms, both of which infect popular distributions of Linux, are two common examples. Given the number of insecure machines on the Net, success is inevitable. The Internet has allowed Trojan horses, viruses, worms, and hybrids (malware that displays the characteristics of two or more of these categories) to propagate farther and faster than ever before.

Beware The Hybrid

Perhaps the most disturbing trend, and the one of which broadband users should be most wary,

is the emergence of *hybrid malware*. This is malware that combines the traits of viruses, worms, and/or Trojan horses. The well-known Melissa virus (which had characteristics of a Trojan horse, a virus, and a worm) was particularly virulent because it could spread via attachments to e-mail, via Microsoft Word documents, or via file sharing.

Magistr/32, ILOVEYOU, Navidad, and others are often called "Trojan worms" because they are activated when a user clicks on an e-mail attachment but distribute themselves via e-mail as worms do. Most such programs rifle your e-mail address book or your saved e-mail messages to find the addresses of potential victims and send themselves to those people's computers in a way that makes them appear to have come from you. Malware that does this, or otherwise attempts to exploit existing relationships between correspondents, is sometimes called a Friends and Family virus), after MCI's famous promotional program for its long distance services. The more the sender respects or trusts you, the more likely he or she is to become the next recipient.

The Hybris worm, on the other hand, does not leverage the reputation of the owner of the infected machine but does watch where he or she browses. It scans all Internet traffic entering or exiting the machine, including Web pages, e-mail, Internet relay chat (IRC), etc., and sends itself to any e-mail address it sees.

Broadband connections potentiate these malevolent programs by allowing them to spread so quickly, once they are activated, that a human being often cannot pull the plug before it's too late.

DDoS Attacks

In an alarming development, malware that doesn't hurt your machine but instead prepares it to join in an attack on others is beginning to surface. Your infected machine appears normal until given a special "attack signal." It then becomes a zombie--a mindless soldier in a distributed denial of service (DDoS) attack. In response to a hacker's marching orders, your machine and others launch as many requests as they can, as fast as they can over high speed connections, at a victim. The goal: to overwhelm and, possibly, bring down a Web server or router belonging to someone the hacker dislikes.

While the attacking machines may be spread throughout the world, the Internet's routers focus the attack--like a lens--on the victim machine and its Internet connection. Most DDoS attacks, to date, have simply been pranks but there is real concern that they could be used as a "cyberwarfare" tactic by terrorists or hostile governments.

The No-Code Plague: E-mail Hoaxes

Finally, there's one type of infection that cannot be stopped by any hardware or software device other than your own brain: E-mail hoaxes. These are not malicious programs that replicate themselves; in fact, they do not replicate themselves at all. They ask you to do the work for them. Akin to chain letters, these e-mail messages sometimes promise riches for forwarding them to others, ask you to save a child in danger or fulfill his or her last wish, warn of a horrible computer virus, or urge you to sign onto an e-mail "petition" promoting a seemingly worthy cause.

The one thing these chain letters--which are always either hoaxes or the results of innocent blunders--have in common is that they ask you to send them to everyone you know. And, given your fast new broadband connection, you can...setting off a wasteful storm of resource consuming e-mail and possibly facing disconnection for violating your Internet service provider's acceptable use policy.

Remember, whenever an e-mail message asks you to pass it on to everyone you know--and especially if it promises you something for doing so--it is invariably a hoax. As the owner of a broadband connection, it is important that you act responsibly and do not propagate such

messages further. After all, not everyone is lucky enough to have as much bandwidth as you. Sending them a copy of a bogus message wastes their disk space and bandwidth and may slow down or even block more important mail. It also may alarm them needlessly.

Spyware: The Threat From Within

As if the threat of malware weren't bad enough, users are also finding their privacy is under attack via programs whose publishers they thought they could trust. This phenomenon is called "spyware". Many programs--including file download utilities, streaming media players, and other programs that are "sponsored" by advertising banners--spy on your actions and report them to their makers.

Even Web browsers may snitch on your Web browsing habits via features such as "What's related," which prepares lists of sites similar to ones you are already visiting. And some versions of Microsoft Windows set an Internet Explorer "cookie" when they're installed. This cookie, which contains a unique identifier, could allow anyone to identify and track you as you visit a growing collection of Web sites and services.

Other spyware attempts to circumvent corporate and personal firewalls by setting itself up as a browser "plug-in." This allows the snooping program to use your browser, which is generally authorized to access the outside world through any firewall, to send information that would be blocked if it were sent by a separate program. This genre of software "browser parasite spyware."

Even if you do not give your real name (or are not asked for your name) when you acquire it, the vendor of a spyware program that reports your activities can still compile a personal dossier on you. It can do this in several ways. It can extract your name from the registration information you typed in when you first installed your Windows operating system or applications. It can find out your e-mail address from your e-mail software--especially if it's a common product such as Microsoft Outlook or Outlook Express. Or it can match your computer's IP address (which changes much less often when you have a high speed connection than if you dial in via a modem) with information you've given voluntarily to any Web site.

Software vendors often claim that the information they compile is not personally identifiable--that is, that they track trends but not individual users. But can they be trusted to keep their promise in the long run--especially in rough economic times or after mergers or acquisitions? And why do their privacy policies seem to be riddled with loopholes, such as clauses giving them the right to change the rules at any time with little or no notice? For example, a typical privacy policy, which at first appears to be very pro-consumer, says the following near the end:

What happens if you change your privacy policy?

Any changes will be posted here before they go into effect.

If you happen to look again months--or even years--later you may find that the company has authorized itself to do things of which you may not approve.

In general, it's important to avoid any software that transmits information about your activities, no matter what promises the vendor makes. It's also a good idea to install utilities that can detect clandestine activities so that you can spot spyware. While spyware affects both low-speed and broad-band users alike, your fast 24x7 connection affords snoops the opportunity to gather much more information about you.

He Sees You When You're Browsing; He Knows When You're Online

You may still be a sitting duck for other forms of espionage even if you've managed to avoid installing spyware on your system or have blocked its attempts to spy on you. You can still be tracked via browser cookies, Web bugs, e-mail bugs, and "active content" (including Microsoft's ActiveX controls and the scripts that can be included in Web pages and in e-mail) as you read your e-mail and go about your daily Web browsing. Those techniques can be used not only to track your activities, but also--in some cases--to take control of your machine.

Web pages and e-mail may have content that compromises your privacy or even renders your system unusable. An HTML message containing an image tag, for example, will cause many e-mail clients to retrieve the image automatically when the mail is read. If your e-mail address (or any other unique identifier) is included in the HTML image tag, a spammer can determine from his or her Web server logs that the address is valid and that the mail was opened. Such an image tag is sometimes called a "mail bug" and might look something like this code example:

```
<IMG SRC="http://images.spammer.com/picture.jpg?clueless@newbie.com">
```

Because the image will be retrieved via HTTP, the server may also be able to place a cookie on your machine if browser software is used to display the mail. The most popular e-mail clients all use browser software to render mail. Outlook, Outlook Express, and AOL use Microsoft Internet Explorer. Netscape Communicator uses Netscape Navigator. Opera uses its own internal HTML rendering software. And Eudora uses Internet Explorer unless explicitly configured not to do so. The user may not know that any invasion of privacy has taken place, especially if the image is an invisible "clear GIF" or Web bug.

A hostile script embedded in a Web page or in e-mail may "take control" of your machine by opening an advertising or pornographic Web page in your browser. It can then prevent you from closing the window or shifting the focus to another window. A malicious script can freeze the browser or the entire machine. A message with intentional formatting errors may crash some vulnerable e-mail clients or infect them with a worm.

Many of these exploits are cross-platform due to the cross-platform nature of HTML, JavaScript, and Java. All of them are also possible via a dial-up connection. However, a 24x7 broadband link makes them more dangerous because they can do their dirty work much faster. You won't have a chance to say, "Hey, my computer shouldn't be dialing the phone now!" and disconnect the line before it's too late.

Fortunately, there's software available that filters out many, if not most, of these exploits. Some is intended for use on a mail server, so if you are not running your own server you'll need to find an mail provider that runs it. Other utilities that defend against malicious content can run right on your own machine. Often, too, they include the pleasant option of filtering out many of the annoying flashing ads that tire your eyes and tax your patience. Many software utilities, **if configured correctly**, block ads, Web bugs, and cookies from sites you don't specifically identify as trusted.

Self Defense

With all of these ghoulies and ghosties waiting to infiltrate your computer via your broadband link, how can you defend yourself? Remember the mnemonic, *TICKLE*, and follow it.

T Is For Test

Test your machine for spyware, viruses, and other hostile software that might already be present.

I Is For Install

Install Firewalls, that is. Hardware firewalls, which are often built into low cost residential gateways, are also useful tools. These products often contain Ethernet hubs or switches, saving you the cost of a separate one. They usually make it quite easy to share a single Internet connection among several computers in your home or office. Their network address translation feature can stop some network attacks cold. But these devices do not block outbound connections made by spyware or malware, and so cannot do the whole job by themselves, so be sure to install an outbound blocking firewall that can recognize rogue applications, too.

C Is For Choose

Choose a Computer Consultant and ISP's that are security conscious. In particular, look for mail providers that can filter e-mail at the server level and can block at least some spam and malware before it ever gets to your machine. Otherwise, you're faced with a take-it-or-leave-it proposition.

K Is For Keeping Up-to-Date

Keep your security software up to date. The overwhelming majority of malware infections can be avoided if the user downloads virus patterns and updates firewall software regularly.

L Is For Learn

Learn about the latest security threats from Symantec's and Microsoft's Web sites and others.

E Is For Educate

Educate others and encourage them to follow in your footsteps. When you receive a copy of a virus, worm, or Trojan horse, let the sender know that his or her computer has run amok and alert his or her ISP's help desk so that the threat can be contained. Warn folks who send you chain letters and hoax viruses that they've been taken in. By doing these things, you can use your broadband connection to improve security rather than becoming a victim.

What to do next?

The primary goal of our whitepapers is to educate. If you feel that you have taken the appropriate steps to protect your computer or your business network then you have nothing to worry about. We ask and hope that you will share this information with others. If you need help then schedule a free consultation.

Our consultants primarily serve the Connecticut and New York marketplaces. Our focus is on small to medium sized companies in addition to home services for executives, telecommuters and anyone with broadband "always on" connections.

Initial consultations are scheduled with a Zeleration senior or junior partner who has a personal stake in the firm. Our goal during an initial consultation is to evaluate and propose solutions to computer problems. Approval of our estimates to complete work is required before work begins.

Please call Justin Higgins at (203) 494-9617 to schedule an appointment or send email to askus@zeleration.com.