

May 15, 2001

Virus vandals target computer networks

Companies must upgrade IT security to stay ahead of hackers' ingenuity

The advance of information technology creates a struggle between those who would harness IT's power for productive purposes and those who would subvert it for crime or mischief. For every advance in computer security comes an attempt to overcome it. "It's always a catch-up game," according to one computer researcher.

Such has been the history of computer viruses, which grew along with the use of computers in the workplace and home and expanded further with the explosion of e-mail. At every step, the ingenuity of the hacker was aimed at fooling, evading or overcoming security measures.

The Internet has opened new vistas for research, communication and commerce, but with the convenience and access come new risks. Information can be lost, stolen or corrupted. According to a group that monitors and responds to virus attacks, information stored on insecure, networked computers is more vulnerable than the same information printed on paper and locked in a file cabinet. Intruders wishing to tamper with the file cabinet have to be physically present. But electronic intruders don't have to be in the same country. Through the Internet, they can invade a computer network and hide evidence of their presence. Companies must learn to protect their electronic assets with the same diligence as their physical assets.

Data recorded by a federally funded center of Internet security expertise show that no business sector is immune from attacks from viruses and related malicious codes like worms and Trojan horses. With so much at stake, the proactive company will keep up with the latest in virus fighting tools.

Hackers have a range of motives—an adolescent playing a joke, a spy seeking information for a competitor, a disgruntled employee after revenge. The goal may be entertainment, challenge, power, attention or financial gain. The scope of the problem has grown along with the Internet.

Computer viruses began to appear in the 1980s, but the number of incidents increased dramatically during the 1990s. According to reports received by the center cited above, from 1995 to 2000, virus attacks increased 800 percent. From 1999 to 2000 alone, the number more than doubled.

In 2000, a worm—a type of virus that replicates itself through e-mail and the Internet—took the problem to a new level of speed and penetration. The Love Bug started with a single computer and zipped around the world, crippling networks and clogging e-mail traffic. Like the Melissa worm of the year before, the Love Bug arrived in a document attached to an e-mail. It invited users to open it with the innocent-seeming subject line: "I love you." This worm then e-mailed a copy of itself to everyone in the address book of the infected computer. Then, more copies went to everyone in the recipients' address books. Without an anti-virus program to block it, the Love Bug spread exponentially, overwhelming the Internet with billions of e-mails.

The attack caused an estimated \$8.7 billion in damage worldwide in lost productivity and costs to restore files. Variants of the Love Bug were still on the loose at the end of 2000.

Spread by mass mail

In February of this year, a computer virus tempted Anna Kournikova fans by posing as an electronic picture of the blonde tennis star. The bug infected thousands of computers by mass mail. A technology company that specializes in anti-virus tools said 10 of its corporate clients shut down their e-mail servers under the deluge.

In March, the "Naked Wife" virus infected more than 30 companies and a U.S. military network. Arriving in an e-mail, the promised pictures were actually a program that deleted vital files before e-mailing itself onward. Curiosity about tantalizing messages or pictures overcomes prudence, which hackers use to their advantage.

In early May, the "Homepage" worm broke out in the United Kingdom. It lured users with: "Hi! You've got to see this page. It's really cool." Once executed, the attached file forwarded the e-mail to the user's address book and opened a pornographic Web page. Homepage spread

(continued on next page)

Virus vandals target computer networks

Companies must upgrade IT security to stay ahead of hackers' ingenuity

(continued from preceding page)

quickly, indicating that many companies still lack basic filtering technology.

Computer viruses share some of the characteristics of biological viruses. They reproduce, they spread, and they need a host. A computer virus attaches itself to a legitimate program in the way that a biological virus takes over the functions of a cell. Execution of the infected program triggers the virus, which then reproduces itself in other programs.

Viruses may enter your system through floppy disks, from downloading from the Internet and from e-mail attachments. Another point of entry is "warez," pirated software that can be downloaded from the Internet. The term "warez," a variant of "software," reflects the youthful computer culture's interest in pushing boundaries with alternative spellings and alternative applications.

Increasing damage toll

Attacks on computers, of which viruses constitute a prominent part, are not harmless pranks. An annual computer crime survey shows an increasing damage toll. Conducted by a computer security organization and the Federal Bureau of Investigation's Computer Intrusion Squad in San Francisco, the survey found:

- 85 percent of organizations responding reported computer security breaches and 64 percent reported financial losses from the breaches.
- The most serious losses were theft of proprietary information and financial fraud.
- Losses totaled nearly \$380 million for the 35 percent of respondents who would quantify, a 43 percent increase over the previous survey.
- By two to one, respondents ranked their Internet connection as the most frequent point of attack.

A West Coast-based research firm estimates the economic impact of viruses worldwide at \$17.1 billion in 2000, a 40 percent increase over 1999.

That impact includes costs to remove viruses from systems and restore files, and the lost productivity resulting from system downtime.

However, a researcher sees a reason for optimism. In 2000, the Love Bug caused heavy damage, but woke many companies up. Alerted by past incidents, corporations increased spending on anti-virus products and on staff. As a result, when the next test came, "the Anna Kournikova bug was bouncing off gateways, not getting anywhere," according to the researcher. Kournikova caused much less harm than it could have. Barring some new virus strain in 2001, the researcher predicts damage from virus attacks will decline 10 percent or more.

Pirated software

Another danger comes from warez, pirated copies of commercial software, which is available for download on the Internet. The installation of unauthorized copies of software is illegal and can be costly to businesses.

Such pirated software is more likely to fail, but carries no warranty. It is also a source for viruses that can damage valuable information. Employees may install the same program on their computers, in violation of the license agreement. In some companies, copying may be deliberate and widespread because the Internet has made it easy to download warez. According to an anti-piracy group, a company that turns a blind eye to this practice is running a risk. Corporations should issue a memo from senior management to all employees on computer software and copyright law. The memo should spell out that unlicensed copying of software is illegal, and that an employee must not copy or download or install any program without permission. The memo should point out that possible liability issues call for stern measures, including possible firing.

Warez can also be the vehicle by which an outside operator gains control of a computer, turning it into a "zombie." The means of control is

the Back Orifice program, which can be worse than a virus. If Back Orifice is running in a computer, a remote operator anywhere in the world can gain access through the Internet and take over. The insidious program can be disguised as a component of what appears to be normal software. Warez could contain the program, another reason to avoid downloading it.

The program runs invisibly and opens an “orifice” into the system. The remote operator can perform most of the functions of the computer without the user’s knowledge. The operator can access files, read e-mail, relay communications, see passwords. The hacker can use the computer to carry out a criminal enterprise. Obviously, such access would be very dangerous for a corporation with sensitive data to protect.

Criminal or terrorist attack

As computer systems have become more powerful and sophisticated, so have the means of attacking them. Security measures must keep pace with this evolution. Intruders now use the power of the Internet to coordinate automated attacks on sites. Their tools are widely available on the Internet; the hacker community shares programs and helps each other improve.

A computer researcher believes the days of amateur virus vandals may give way to criminal or terrorist attack. The success of amateurs in overcoming defenses and causing damage attracts the attention of those with a more sinister purpose.

Newt Gingrich, former speaker of the U.S. House of Representatives, has warned that enemies of the United States could launch a “cyber Pearl Harbor” sneak attack. Such an attack “of mass disruption” could block communications, cause electrical blackouts and snarl financial transactions. Compared to the cost and complexity of creating nuclear, chemical or biological weapons, achieving the hacking skill to launch a cyber attack is less challenging. Viruses designed to clog networks or corrupt sensitive

files could be a major part of such an attack by criminal organizations, terrorist groups or foreign nations.

Companies must prepare

A computer security expert warns that technology exists to aim a virus at a particular corporation. Instead of being unleashed to strike at random, a virus-infected e-mail could be used for industrial espionage, targeting a specific person in the corporation. Once the attachment was opened, the virus could access whatever the computer user could access, copying files and transmitting them.

In addition to external attack, companies must prepare for internal threats. In a time of economic uncertainty, with layoffs increasing, companies must worry about disgruntled employees seeking redress through a computer attack.

To fight back, corporate security and IT departments should strengthen their electronic defenses:

Anti-virus programs. This software, available from a variety of manufacturers, checks the computer for problems. At a minimum, the program must scan the following:

- all incoming e-mails;
- all programs before they are installed;
- all files as they are read from or written to a storage device;
- all files on the computer at least once a day.

Ideally, an incoming e-mail would be checked once at the gateway and again at the desktop. With a good anti-virus program, a subscription service should keep the virus signature database up to date. A virus checker looks for specific signatures, reacting when it recognizes one.

Firewalls. They form a first line of defense against an unauthorized user gaining access to a private network, serving as gatekeepers. Firewalls can

(continued on next page)

Virus vandals target computer networks

Companies must upgrade IT security to stay ahead of hackers' ingenuity

(continued from preceding page)

selectively block the ports to the computer, allowing only benign traffic in and keeping hackers out. As with anti-virus programs, firewalls must be updated to stay abreast of hacking ingenuity.

E-mail filter. This acts as a missile defense shield against incoming e-mail, allowing an organization to automatically screen e-mail for content. The filter not only blocks obscene e-mail, but also ensures that no attachments arrive carrying a virus. For example, Homepage, Love Bug, Melissa and other attackers would have been stopped by an e-mail filter with appropriate policies installed.

Beware of warez. Web-filtering software should block warez. Using warez is risky, illegal and unethical. Companies should consider an addition to their ethics policy forbidding the use of illegally copied software. The downloading and use of warez on company equipment should be grounds for disciplinary action. Companies should only buy software from vendors they know.

Statement of policy. Corporations should have clear guidelines on safe computer use and make sure employees are aware of them. Anti-virus software experts recommend these rules:

- Do not run, download or forward any unsolicited documents or executable programs. Everything must be virus-checked first.
- Treat e-mail with suspicion. Be very wary of attachments.
- Do not unload executables or documents from the Internet.
- If in doubt, ask the IT department before opening the file or e-mail.
- Send virus warnings to the IT department for verification. Hoax warnings waste time and energy.

- Back up important files on a separate medium, such as a diskette.

Management should reinforce these guidelines with periodic reminders. A survey by an anti-virus company in Great Britain found that 37 percent of business e-mail users would open an e-mail with a Love Bug-type invitation. This laxity comes despite repeated warnings and knowledge of the damage the original caused.

Our society depends on motor vehicle traffic. We try to make that traffic as safe and efficient as possible. Stop lights and speed limits regulate the flow.

Likewise, corporations must make computer traffic as safe and efficient as possible through anti-virus tools and establishing rules of the high-technology road. It makes no sense to invest in the latest computer technology without investing in the means to protect it.

IT security begins with a recognition by top management that proprietary information, profits and prestige are at stake. A technically proficient security service provider can assess vulnerability and recommend solutions. Virus-fighting software and staff should be kept up to date. Educating employees on the commitment to information security makes it a part of the corporate culture. Written guidelines and regular reminders reinforce this commitment.

Computer viruses threaten the confidentiality, integrity or availability of corporate information. Just as society inoculates against a biological virus to contain its spread, a forward-looking, astute company will inoculate against the viruses that attack computers.



The Lipman Report Editors