Next-Generation Viruses Present New Challenges

John Edwards

Computer technology has advanced in many ways, but not all of them have been welcome. One of the more undesirable has been the ongoing advance of virus technology.

Taking advantage of emerging computer technologies and techniques, virus writers come up with new ways to defeat existing security software, infect computers, cause damage, and spread their malicious creations. This has become evident recently with the emergence of several innovative and potentially harmful viruses.

A decade ago, viruses were relatively easy to find and fix, and they spread slowly, generally by floppy disks or LANs. Now, however, increasingly creative authors are exploiting the Internet, open-source software, peer-to-peer technology, and other developments to write viruses, worms, and Trojan horses that invade computer systems in new ways, propagate around the world quickly, and wreak havoc on victims.

New viruses arrive with such speed, thanks in part to the Internet, that even antivirus experts frequently aren't aware of them until thousands of computers have been infected, said Michael Rasmussen, a security analyst for Giga Information Group, a market research firm, and also a director of the Information Systems Security Association, a nonprofit organization of IT security professionals.

Besides spreading more quickly than their predecessors, the latest crop of viruses is also much better constructed. "Early viruses were usually crude and were easily understood and eradicated. Today's virus writers develop carefully crafted code that is designed to exploit the smallest flaws in system and application software," said Paul Zimski, a researcher at Finjan Software, a computer-security application vendor.

REMOTE-CONTROL VIRUSES

A new generation of viruses infects machines not only by using their own code but also by linking to and accessing malicious code from newsgroups or Web sites.

Hybris

Security experts consider Hybris to be particularly sophisticated and dangerous.

Hybris, a Trojan horse/worm hybrid that surfaced last year, spreads by attaching itself to a user's outgoing e-mail. Then, said Kenneth van Wyk, chief technology officer for Para-Protect Services, an IT security firm, "It connects itself to the alt.comp.virus newsgroup to receive updates." These updates revise Hybris' malicious capabilities, which so far have involved only the placement of messages or spiraling graphics on victims' screens.

Therefore, Hybris' real danger is that the code could suddenly use new plug-ins to become very destructive. "We don't know what the next plug-in will do," said Vincent Gullotto, director of research for Network Associates' McAfee antivirus subsidiary. "Hybris could suddenly become dangerous and quickly spread itself through machines that haven't yet been cleaned of the code."

The code Hybris downloads from the newsgroup is encrypted, which can help hide its contents from antivirus products. Although antivirus vendors broke the encryption on Hybris' original code, this may not protect against encryption used in future updates.

As Figure 1 shows, when the recipient opens the attachment and activates the malicious code, Hybris patches its code to the WSOCK32.DLL file, the dynamic link library that implements an application's Windows Socket application programming interface.

The viral software then uses several Windows Socket data-communications functions to scan e-mail addresses from incoming messages and from the Web pages and newsgroups the user visits. Hybris then sends itself from victims' computers to any valid address transmitted over their e-mail connections, as well as addresses that were part of a visited Web page or newsgroup.

"Recipients think the message is from someone they know, and they wind up with Hybris," said Pete Privateer, president of Pelican Security, a software company.

Although Hybris is complex, all leading antivirus vendors have developed antidotes. Hybris has infected tens of thousands of computers worldwide. "It's impossible to tell exactly how many, since users often download the [antidote] software and solve their problem without reporting it to anyone," said van Wyk.

By following e-mail addresses and names embedded within the software, security experts traced Hybris to a group of Brazilian hackers. Experts haven't determined the author's real name yet because the group is secretive and members use online pseudonyms.

Davinia

Although security experts defeated the VBS.Davinia.B worm, it still served as a proof of concept for future types of malicious code that could be very dangerous and destructive.

Davinia functioned only on computers running Microsoft Outlook without the Office 2000 UA Control patch, which corrected an ActiveX-related vulnerability.

Victims contracted VBS.Davinia.B via an infected e-mail message. The message had no subject line and appeared blank but actually contained HTML code that didn't generate text or images on users' screens.

If victims had active Internet connections, the code started their Internet Explorer browser and downloaded and opened a Microsoft Word 2000 document from one of two Web sites the worm's author set up. The document contained a Visual Basic Script (VBS) macro virus that created a Littledavinia.vbs file in the victim's Windows System folder.

The next time the user booted up, the computer executed the VBS file. The macro sent an infected e-mail message to all contacts in the victim's Microsoft Outlook address book. It then searched for all files on the victim's local and remote drives and overwrote them with HTML code. The code subsequently displayed a message in Spanish, customized with the victim's name and e-mail address, about the author's love for a woman named Davinia.

Antivirus vendor Symantec counted about 100 Davinia victims before security experts shut down the worm after a few days, said Vincent Weafer, director of the company's research center. Experts ended the threat by tracking down and closing the worm's two supporting Web sites. However, they did not locate the author.

"The virus, while innovative, wasn't a big threat to users," said McAfee's Gullotto. "It would have been a bigger threat if it had downloaded its updates from a newsgroup, rather than a Web site, which can be tracked down and closed." Newsgroups cannot be shut down, although Internet service providers can block their transmissions.

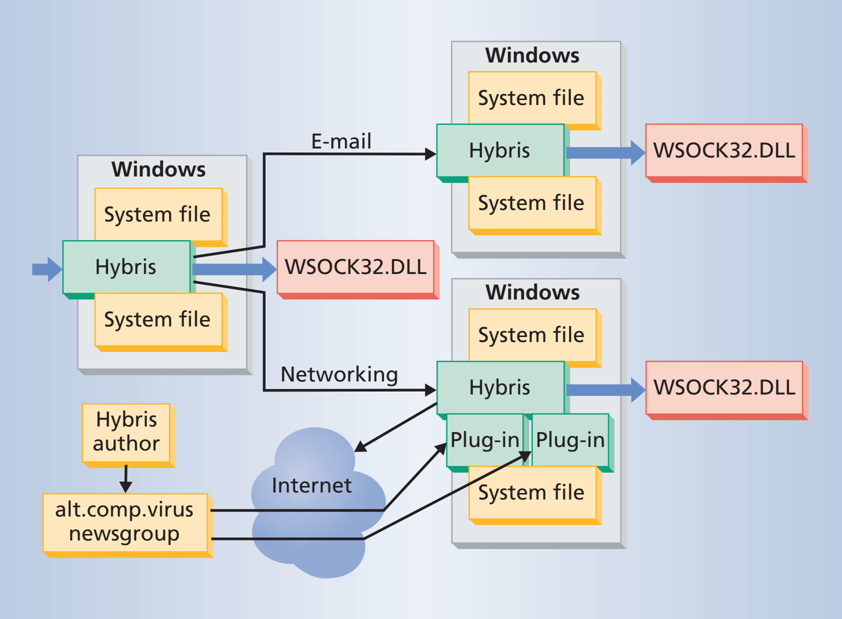

Figure 1. Upon activation, Hybris attaches itself to Windows' WSOCK32.DLL file, the dynamic link library that implements an application's Windows Socket API. Hybris uses Windows Sockets functions to scan e-mail addresses that victims receive and Web pages they visit. Hybris then spreads by e-mailing itself to the victims' addresses. Hybris can also connect via the Internet to the alt.comp.virus newsgroup to update its malicious capabilities.

PEER-TO-PEER WORM: GNUMAN

The W32/GnumanWorm, also called Mandragore, affects computers that access the open-source Gnutella peer-to-peer (P2P) file-sharing system or Gnutella-compatible software such as Gnotella, BearShare, or LimeWire. These systems are often used to exchange music and video files.

Gnuman is one of the first types of malicious code to affect the increasingly popular P2P technology, which lets machines share files and otherwise communicate directly, without a central server.

The worm, which first surfaced last February, attaches itself to the Gnutella client on a user's PC via TCP/UDP port 99, used for some file transfers.

Gnuman, which can be recognized by its 8,192-byte file size, monitors the Gnutella traffic stream for requests from other users for media files. When another user requests a file from an infected computer, Gnuman returns a viral file with the requested name and often the characters "mp3," as in the MP3 compression technology frequently used for exchanging music online. This encourages the victim to download and open what appears to be a media file. Once opened, Gnuman drops a copy of itself as GSPOT.EXE into the victim's Windows Startup folder. The code is relatively harmless and does little more than use up system resources.

"It's a proof-of-concept worm that's designed to highlight Gnutella's vulnerability," Symantec's Weafer said. However, he expressed concern that future Gnuman-like worms may include a more destructive payload.

"Fortunately," he said, "these types of codes don't spread quickly because they don't replicate automatically. They require an inattentive user to actively download them."

OPEN-SOURCE VIRUSES

Virus writers have most often targeted Windows and other Microsoft software, primarily because their popularity gives authors the best chance to cause the most damage. However, with Linux and other open-source software becoming increasingly popular, it was just a matter of time before they also became targets.

In fact, Finjan's Zimski noted, about 50 Linux viruses have been identified since Ramen's arrival earlier this year.

Ramen

Ramen, named after the Japanese noodle soup, was the first major malicious-code threat to Linux machines. Until then, users believed Linux was secure because it was open source and underwent ongoing review and improvement by many developers, said Joe Hartman, director of US virus research for antivirus software vendor Trend Micro.

From a host computer, Ramen automatically scans the Internet for servers with one of three vulnerabilities. The scanning process alone causes problems because it uses considerable bandwidth.

In one approach, Ramen targets a weakness in WU-FTP servers (a popular type of FTP server). The hacker can exploit the weakness using a *site exec* command that runs scripts and coerces the WU-FTPD daemon to execute arbitrary code and give the hacker root access.

A second technique targets a vulnerability in the RPC (remote procedure call) server's rpc.statd NFS (network file system) file-locking status monitor. Ramen gains root access by making insecurely structured calls to the server's *syslog* function, used to log network events.

Ramen can also exploit the *LPRng print spooler service*, which manages the printing process, again using the syslog function to gain root access in Red Hat Linux 7 installations.

Once Ramen gains root access, it initiates a *synscan*, which checks networks across the Internet for open connections to find new host targets such as Red Hat Linux 6, 6.2, and 7 servers.

The worm subsequently replaces the root page of the Web site that the victimized server hosts with an HTML file that shows a box of noodles and says, "RameN Crew looooooooooooooves noodles." When the server next boots up, Ramen scans the Internet for more hosts.

Ramen didn't spread widely before antivirus-software vendors developed an antidote. Said Symantec's Weafer, "Only a few thousand Linux servers were affected. But Ramen proved that even Linux users aren't safe."

Lion and Winux

In mid-March, two more potentially dangerous Linux viruses arrived: Lion and Winux.

Lion. From a host server, the Lion worm scans the Internet for Linux servers running versions of BIND (Berkeley Internet Name Domain) software, used for domain-name server systems, that were not patched for a vulnerability that appeared in January.

As Linux becomes more popular, virus writers are increasingly targeting the open-source OS.

Once Lion finds such a server, the worm uses the vulnerability to infect the machine, steal the BIND password file, and send it to an account unwittingly hosted (and since shut down) by the http://www.china.com Web site. Lion then installs other hacking tools that help it scan the Internet, find other vulnerable systems, and steal password files.

"It has a very nasty payload that basically requires victims to rebuild their systems from scratch," said Finjan's Zimski.

The only defense against Lion is to upgrade vulnerable BIND implementations.

Winux. Winux was the first virus able to infect both Linux and Windows platforms. Winux's author sent the software by e-mail to antivirus vendor Central Command as a proof-of-concept virus containing no payload. Because of its potential to carry malicious payloads, Zimski said, "It definitely doesn't bode well for the future."

Winux can replicate and infect executables on systems running Linux or Windows 95, 98, 2000, Me, or NT. It uses various API functions to find and overwrite files. For example, the virus uses several API functions to overwrite the *reloc* section of Windows executables, where the system stores relocatable code, software whose execution address can be changed.

On Linux systems, the virus overwrites instructions at the start of executables and leaves the Winux code stored at the end of the files. When a user runs an infected application, the virus code takes control, spreads to other Linux executable files, and returns control to the original host file.

BATTLING THE NEW VIRUSES

Combating next-generation viruses requires ongoing vigilance and basic security practices, such as running and updating antivirus applications.

Meanwhile, antivirus-software vendors are developing innovative capabilities for their products. For example, new software from vendors such as Finjan and Pelican Security requires users to define which actions they will and will not allow on a computer or network. "So if a machine suddenly starts sending hundreds of e-mails, for example, the software knows that something strange is going on and notifies the user or network administrator," said Elias Levy, chief technology officer for SecurityFocus.com, which runs an IT security information Web site.

Meanwhile, because most new viruses arrive by e-mail, a growing number of organizations are outsourcing their e-mail services to companies, such as Network Associates, that scan incoming messages for suspicious code.

New viral threats will become even more complex as authors gain additional experience. "The state of the art is being pushed forward for all software, including viruses," said Todd Miller, an analyst with Yankee Group, a market research firm.

Meanwhile, new products and their accompanying security gaps will also pave the way for fresh viruses, Trend Micro's Hartman said.

"We'll never get rid of viruses or virus writers," added Levy. "The best we can do is hope that the virus authors never get too far ahead of the virus fixers." ✷

John Edwards is a freelance technology writer based in Gilbert, Arizona. Contact him at jedwards@john-edwards.com.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org