

Instant Messaging: A New Target for Hackers

Neal Leavitt

Instant messaging is exploding as a means of personal and corporate communications. Individuals chat via IM; companies rely on beefed-up versions of the technology, with its real-time capabilities, for collaborative design work; and e-businesses use IM to provide live, immediate customer service to shoppers.

Market research firm IDC estimates that by 2008, more than 506 million people worldwide will use an IM product. The Radicati Group, another market research company, predicts that there will be 78 million enterprise IM users by the end of 2008.

Meanwhile, the technology is finding its way onto mobile devices, including PDAs and smart phones.

However, as IM becomes more popular, particularly for businesses, it has also increasingly become the target of attacks, such as those using malicious code and phishing.

“Over the past several months, IM viruses and worms have grown an astronomical 1,600 percent compared to last year,” said Jon Sakoda, chief technology officer for IM software vendor IMlogic.

Attacks against major IM networks rose almost 400 percent from five during the first quarter of 2004 to 24 during the same time period this year, according to IM security vendor Akonix Systems.



Some security experts say IM is a following the same patterns shown during the development of e-mail attacks. These include the use of tricks to encourage victims to click on virus-laden attachments or hyperlinks to Web pages that upload applets to either infect visitors with malware or drop unwanted software on their computers.

“Most of this,” Sakoda said, “is relatively benign adware or spyware, but there have been several IM worms that have attempted to shut down security software and disable system applications.”

The most dangerous part about the attacks is their speed of propagation, caused by IM’s real-time capabilities, he noted. According to Eric Chien, principal software engineer for antivirus vendor Symantec, the company ran a simulation in late 2004 that showed IM viruses could spread to 500,000 machines in less than 30 seconds.

Traditional antivirus technology, in which vendors typically need 24 hours

to find remedies for new malicious code, may be too slow to prevent many IM attacks from spreading rapidly.

GROWING PROBLEM

The IMlogic Threat Center (http://imlogic.com/im_threat_center/index.asp)—a consortium of security and IM providers such as AOL, McAfee, Microsoft, Symantec, and Yahoo—said 82 percent of IM attacks included virus or worm propagation.

According to the Center, 64 percent of attacks targeted Microsoft’s widely used systems, particularly MSN Messenger, 11 percent hit Yahoo Messenger, and 25 percent affected AOL’s AIM and ICQ systems.

In June, noted IMlogic’s Sakoda, hackers began shifting focus to AOL, but MSN is still a favorite because of the Microsoft connection and the widespread distribution of the Windows messenger client on PCs.

Also, explained Symantec’s Chien, “Microsoft provides a well-documented API for MSN Messenger that allows one to control it and thus send out worms via IM.”

“For virus authors who want their 15 minutes of fame or criminal organizations that want the largest cash cow, then Microsoft is the biggest animal to run down,” said Jamie Lyndon Yaneza, senior antivirus research consultant for TrendLabs, a subsidiary of antivirus company TrendMicro.

Driving forces

Hackers have the same incentives—such as financial gain, enhancing their reputation among peers, solving a technical challenge, and creating mischief—to attack IM systems as they do to target e-mail or other network-based technologies.

However, e-mail has been a more attractive target than IM for many years. Popular public IM systems such as AIM and Yahoo Messenger are closed and thus don’t generally connect to other systems. This limits IM’s ability to spread attacks. Also, until recently, IM clients have been simple

systems with few published vulnerabilities to exploit.

In addition, IM protocols are proprietary, which has made them more difficult to reverse engineer, explained Ero Carrera, a researcher at antivirus-software vendor F-Secure. E-mail, on the other hand, uses publicly available standards such as the Simple Mail Transfer Protocol (SMTP), he noted.

However, after years of e-mail attacks, users and security firms have shored up their defenses. Hackers have thus turned their attention to IM, said TrendLabs' Yaneza.

He added that IM's informality and immediacy causes many users to let their guard down when using the technology, something that is not the case with e-mail, whose risks are better known.

And adolescents, who comprise the fastest-growing segment of IM users, don't generally practice safe computing as much as adults, said Craig Schmugar, virus research manager for antivirus company McAfee.

Meanwhile, as IM's functionality has increased, systems have become more complex and vulnerabilities have crept in.

IM vulnerabilities

As a messaging system, IM suffers from many of the same vulnerabilities as e-mail. For example, IM users can launch a hacker's attack by inadvertently opening infected attachments.

Users can also click on a hyperlink in an instant message that leads them to a phisher's counterfeit bank or e-commerce Web site. The site asks them to enter their user name, password, bank account and Social Security numbers, and other personal information that hackers can subsequently sell or use illegally.

In addition, IM supports the peer-to-peer transfer of files and messages with attachments, so they bypass most of e-mail's server- and security-gateway-based virus scanning.

Password protection is limited in most IM systems, and the communica-

tions are rarely encrypted. "Without encryption, any off-the-shelf sniffer can reveal the content of IM communications," said Marcus Sachs, a computer scientist at SRI International, a contract research institute, and deputy director of the US Department of Homeland Security's Cyber Security R&D Center.

As IM has grown more popular, it has become the target of attacks.

Unlike e-mail, which usually uses SMTP and TCP/IP port 25, IM systems use various ports and proprietary protocols. For example, AIM and ICQ use port 5190, MSN Messenger uses port 1863, and Yahoo Messenger uses ports 80 and 5050. This lack of consistency makes it difficult for IT departments to monitor IM communications for attacks and threats.

No corporate IM policies

IM problems are caused not only by common coding mistakes but also by a lack of corporate IM-use policies. A survey of US businesses by SurfControl, a corporate Internet security vendor, found that 90 percent of respondents had an Internet-access policy but only 51 percent had an IM policy.

Many companies don't recognize IM's dangers, noted Tim Johnson, director of the IMlogic Threat Center. And many organizations that don't use IM for corporate communications aren't aware that employees are using the technology on their own, as they can frequently download popular IM systems from the Web themselves.

IM ATTACKS

IM attacks are like those that affect e-mail and other types of network-based assaults.

Malicious code

IM attacks have included various types of Trojan horses and worms.

Assiral.A This simple mass-mailing worm arrives as a Windows 32-bit executable that deletes files and modifies Internet Explorer home-page settings.

Bizex. The main component of this worm, which attacks ICQ systems, has spying and data-stealing capabilities. Bizex spreads by sending a hyperlink to a victim's contacts. Clicking on the link sends them to a Web page that uploads the worm.

Bropia. This worm and its variants, including Kelvir and Serflog, spread via MSN Messenger. They copy themselves into a Windows system directory, download more malware onto the victim's computer, and reduce system security. Some variants hide on a PC, only to re-emerge at a later date.

Buddypicture. The attack by this Trojan, which affects AIM systems, starts with an instant message that includes a hyperlink to a Web site supposedly featuring pictures of the purported sender, whose name was on the victim's contact list. The message asks the victim to download an applet first. If downloaded, the applet uploads adware and spyware to victims' computers.

Gabby.a. The Gabby worm attacks AOL's AIM and ICQ systems by sending recipients a hyperlink and tricking them into clicking on it. Victims then get to a Web page that uploads spyware, as well as a worm that opens a backdoor to the machine and eliminates Windows services such as those used with antivirus and firewall software.

Kelvir. This worm spreads by sending a hyperlink to MSN Messenger users with messages such as "Hey, check this out" or "LOL, this is a funny picture of me." Users who click on the link go to a Web page that uploads the virus to their computers. Kelvir then spreads via victims' buddy lists.

The worm can turn computers into spam broadcasters, log keystrokes such as those in user names and passwords, and e-mail the information to hackers.

Kelvir recently shut down international media company Reuters' pro-

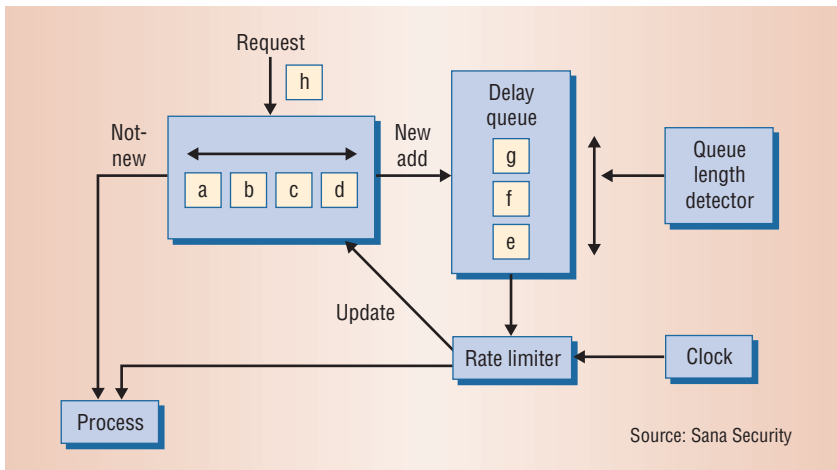


Figure 1. When a security system spots worm-like behavior on an IM network, virus throttling slows the spread of the malware and thus limits the damage. The technique compares a new connection that an IM client is trying to make—in this case to h—to a short list of frequently made, and thus presumably safe, connections—in this case a, b, c, and d. If the new connection is on the list, the system lets it pass. If it is a new connection, the system places it on a delay queue, which in this case already holds messages to e, f, and g. If there is a lot of traffic to many different destinations, as occurs with a virus, the delay queue gets large and the system stops further transmission.

proprietary, closed, 6,000-user IM system, which is based on Microsoft technology.

Phishing

IM phishing is an industrywide issue. For example, phishers recently attacked Yahoo Messenger by sending a message containing a hyperlink to a counterfeit Yahoo Web site. The site displayed a sign-in screen and asked victims to log in with their user ID and password. With this information, an attacker could sign in to the victims’ Yahoo Messenger accounts and hack into their contact lists and user profiles, which can contain personal and financial information.

According to Yahoo Messenger director Frazier Miller, the company has enhanced security by adding a new SpamGuard feature that lets consumers report spam or unsolicited IM messages. In addition, it blocks communications from previous senders of unsolicited messages. The company also started the Yahoo Security Center (<http://security.yahoo.com>), which educates consumers on how to protect themselves online.

Hijacking

IM worms can let an attacker hijack and send messages with infected attachments or phishing-related hyperlinks from victims’ clients to their IM contacts.

This could make the contacts believe the communications came from an acquaintance and that opening attachments or clicking on hyperlinks is safe.

Denial-of-service attacks

An attacker could launch a DoS attack by sending many specially crafted TCP/IP packets to servers in an IM provider’s infrastructure and thereby prevent legitimate messages from passing through.

Hackers could also send many packets to an IM user to hang up or crash the messaging client or eat up CPU resources and destabilize the computer.

ADDRESSING THE THREATS

Messaging providers and security companies are taking steps to combat IM attacks, such as establishing the IMlogic Threat Center, which monitors and analyzes IM security risks,

warns users against vulnerabilities, and provides threat management. Its members include about 25 companies, which fund the organization, and about 400 individuals.

IM providers and security companies also advocate educating consumers about safe computing practices.

Upgrading IM technology

IM attacks can cause buffer overflows, which occur when a program or process tries to store more data in a buffer than it was designed to hold. The extra information overflows into adjacent buffers, corrupting or overwriting valid data. The overflowing data can contain instructions designed to cause problems such as client failure or the consumption of CPU or memory resources.

Poor programming and memory management can enable buffer overflow attacks. Thus, major IM networks are revising their clients to ensure better memory management.

Sana Security’s Primary Response protects against buffer overflows by preventing the type of code execution that occurs during the attacks.

Primary Response also includes a profile of normal file and network activity so that the system can detect anomalous behavior that indicates an IM-based or other attack. The product also includes Sana’s Active Malware Defense Technology, which recognizes programs behaving maliciously.

Firewall maker Zone Labs makes IMSecure, which can detect viruses; block spam, IM-borne scripts, and buffer overflow attacks; and encrypt data being sent to another IMSecure user. Users can also choose to block certain IM features, such as file transfers.

Symantec and McAfee added IM scanning and the ability to remove malware from attached files to their Norton AntiVirus and VirusScan products, respectively. And TrendMicro’s InterScan Web Security Suite filters Web traffic for the URLs of Web sites known to be involved in malicious downloads, phishing, and spam.

To limit the damage that infected files can cause, Microsoft has designed MSN Messenger so that it won't transfer several types of files, such as executables, command files, and program information files (which tell Windows how to run non-Windows applications).

Meanwhile, vendors are starting to release end-to-end encryption plug-ins for IM clients.

IM-use policies

"Companies need to have a policy on IM, even if it's to ban it," said SRI International's Sachs. "The best policy is to provide for a way that employees can use IM safely and describe how the technology will be used [only] to support business needs."

According to SurfControl, IM-security policies could limit which users can access IM networks; route instant messages through the secure enterprise network; require regularly updated, real-time message-content filtering; mandate virus scanning of all file transfers; and block transmission of hyperlinks over IM.

Slowing IM worms' spread

Traditional antivirus technology reacts too slowly to stop many IM virus outbreaks. *Virus throttling*, a promising alternative that is still experimental for IM, slows the spread of messaging worms and thus limits their damage, rather than prevent the infections, as Figure 1 shows.

When a system spots worm-like behavior on an IM network, virus throttling limits the number of IM messages an infected user can send outside the small group of contacts with which they communicate most frequently, explained Matthew Williamson, a Sana Security senior research scientist who developed the technique while at Hewlett-Packard.

Said Trend Labs researcher Ivan M. Macalintal, "Attacks will increase in sophistication." For example, IM malicious code will make

itself harder to detect by mutating several of the elements that security systems use to identify it. For example, the malware may mutate the code itself to defeat the code signatures that antivirus software uses to detect malware, noted the IMlogic Threat Center's Johnson.

And in the near future, said F-Secure's Carrera, wireless-IM security problems may arise.

IM's rapid growth in the enterprise and lack of deployed IM security technology continue to make it attractive to attackers. "IM has become an infection vector alternative to e-mail, and we will see a gradual increase of threats simply because of the bulk of users,"

said Jim Murphy, SurfControl's director of product marketing.

According to Murphy, large organizations will be slow to react to the threat but eventually will be compelled to do so by the risks involved.

Neal Leavitt is president of Leavitt Communications, an international marketing communications company based in Fallbrook, California. He writes frequently on technology-related topics. Contact him at neal@leavcom.com.

Editor: Lee Garber, Computer,
l.garber@computer.org