Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Instant Messaging Menace: Security Problems in the Enterprise and Some Solutions

In this paper, the security threats posed by the use of consumer grade instant messaging clients in the enterprise, including privacy and identity issues, and malware and bug vulnerabilities, are discussed. A course of action to include creation or revision of written security policies, installation of antivirus protection at the gateway and on all servers and desktops, determination of requirements for secure instant messaging, and tightening of the company firewall to block consumer grade instant messaging clients is...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

The Instant Messaging Menace:
Security Problems in the Enterprise and Some Solutions.

Dan Frase
GSEC – GIAC Security Essentials Certification
Assignment version 1.3
CDI East: November 27 - December 3, 2001
(Washington, DC)
Original Submission

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Abstract

The security threats posed by the use of consumer grade instant messaging clients in the enterprise, including privacy and identity issues, and malware and bug vulnerabilities, are discussed. A course of action to include creation or revision of written security policies, installation of antivirus protection at the gateway and on all servers and desktops, determination of requirements for secure instant messaging, and tightening of the company firewall to block consumer grade instant messaging clients is recommended.

Introduction

Instant messaging (IM for short) isn't an application that was developed for use in the workplace. It was developed as a tool to enable home users to see when their friends are online, and to provide a way for people to converse with their "buddies" in real time, and provide a medium for chatting and for the direct exchange of URLs and files. According to one writer, "it was an online toy originally used mainly for dating and cyber sex" (Langa). But as its popularity caught on with home users, some started to see merits for the applications' use as a business tool due to its ability to allow immediate contact with co-workers, clients and vendors, and enable call center personnel to answer online shoppers' questions in real-time, as well as acting as a valuable collaborative tool. And so they installed the clients - oftentimes without the IT departments' knowledge or blessing – on their company computers. Without realizing it, they opened their corporate infrastructure to a myriad of security threats including privacy issues (personal information leakage, IP address exposure, loss of confidential information, and eavesdropping), identity issues (impersonation), malware in transferred files (worms, viruses, Trojan horses, and other malicious software), and security bugs in the clients such as buffer overflows that could expose users to any number of different types of attacks (denial of service attacks, worm infections, privilege-elevation attacks, Trojan attacks, etc.).

Statistics regarding the growing use of IM in the workplace can be found in recent reports by Jupiter Media Metrix, International Data Corporation (IDC), Forrester Research, and Gartner, Inc. According to Gartner, instant messaging will be the core of wireless e-commerce, live collaboration, virtual gaming and a host of other Internet applications (Gartner, Inc. Press Release, May1, 2001). Gartner also estimates that free IM services will be found in 70 percent of enterprises by 2003, and it will be implemented by end-users without IT organization sanction or support (Gartner, Inc. Press Release, October 11, 2001).

It's evident that the majority of enterprises will face the security problems caused by IM's usually unwelcome and unchecked entry into the workplace. The best course of action for IT managers is to stop this trend in their organizations before it becomes completely overwhelming. Establishing, distributing and enforcing security policies is the first step, followed by making sure that antivirus protection is installed and frequently updated on gateways, servers and desktops, then determining the need for secure IM solutions, and finally tightening up the firewall (Berg, p.49). Software auditing may also be necessary to enforce security policies since IM clients are very good at bypassing efforts to block them.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The first step in understanding the threat posed by the use of consumer-grade IM applications in the enterprise is in knowing the features of the top four IM clients that commonly infiltrate the workplace.

The Big Four IM Clients

Currently, the four most popular IM clients are AOL's AOL Instant Messenger (AIM) version 4.7 with 100 million users, AOL's ICQ version 2001b with 122 million users, Microsoft's MSN Messenger version 4.5 with 42 million users, and Yahoo! Messenger 5.0 with an undisclosed number of users. The breakdown of features is shown in Table 1. All four are free and readily available for downloading.

IM Client	One-on-One Messaging	Multi-user Chat	Voice Chat	PC-to-Phone Voice Chat	Video Webcam Chat	Handheld Connectivity (PDAs)	File Send & Receive	Directory Sharing	Ad Banners
AIM 4.7	X	X	X	X		X (AOL members)			X
ICQ 2001b	X	X	X	X		X	X	X	
MSN Messenger 4.5	X	X	X	X		X	X		X
Yahoo! Messenger 5.0	X	X	X	X	X	X	X	X	

Table 1. Features of the Top Four IM Clients.

All four of the top IM clients allow users to see when anyone added to their contact or "buddy" list is online and available for messaging, chatting, or file or URL sharing. All allow one-on-one messaging, multi-user chatting, voice chatting, and PC-to-phone voice chatting. Yahoo! Messenger 5.0 also allows video webcam chatting. All allow for instant messaging with handheld devices (PDAs), but AIM 4.7's service is only free to AOL members. All but AIM 4.7 allow users to send files to, and receive files from, other users. But ICQ and Yahoo! Messenger also allow a user to share a directory of files. And, as an added bonus, AIM 4.7 and MSN Messenger 4.5 users get to view ad banners while they use their clients. Many users find this last feature annoying.

Another aspect that many users of AIM find irritating is the lack of an option to approve or reject other users' efforts to add them to their buddy lists (Ryan, p.36). This privacy issue could possibly increase the security threat presented by newer worms like Goner.A (which used the ICQ contacts list to replicate) that have the ability to use IM contact lists to infect online contacts. Since AIM doesn't restrict anyone from adding anyone else to their buddy lists, the potential for worms to spread using the AIM client contact list increases.

Some limitations of MSN Messenger 4.5 are that it doesn't save IM conversations, and it doesn't allow you to send a message to someone who isn't online. Although MSN Messenger 4.5 doesn't include video chat capabilities, the Windows XP flavor, Windows Messenger, does. Windows Messenger 4.0 is built into Windows XP. Version 4.5 of Windows Messenger is available for download.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

None of the four IM clients are compatible with each other - yet. If a user wants to keep tabs on friends that use different IM clients, they have to install more than one client. Microsoft and Yahoo have been urging America Online to foster interoperability and formed IMUnified as a coalition to develop open standards. America Online has been reluctant to open its network to subscribers of other services, but that's likely to change. As a condition of AOL's January 2001 merger with Time Warner, the Federal Communications Commission insisted that the company show progress toward opening its instant messaging networks to competitors (George and Swanson). Also, Microsoft and AOL are expressing support for a new interoperability protocol under development by the IETF called the Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) standard. When all four IM clients build support for the SIMPLE protocol into their clients, IM could become as ubiquitous as e-mail is today.

But SIMPLE won't be sufficient to prevent Internet bandwidth problems in the near future. If leading IM service providers such as AOL and Microsoft offer multimedia instant messaging services (instant messages with audio or video clips attached) to their millions of users, Internet communications could grind to a halt. The Internet Engineering Task Force (IETF) is soliciting potential fixes from its participants (Marsan). The problem is due to an inherent problem in the protocol SIMPLE is based on, Session Initiation Protocol (SIP). SIP runs on either TCP or UDP and there's no way to keep it from using UDP, which has no built-in congestion controls like TCP does.

Security Threats

Privacy Issues

Privacy threats caused by IM clients in the workplace include personal information leakage, IP address exposure, loss of confidential information, and eavesdropping. The same personal information that users either don't mind, or are unaware of, sharing with the world when they sign up for IM services at home becomes a more serious problem in the workplace. Companies may not want their employees sharing personal information - including company e-mail addresses - with the Internet community. Users may end up sharing even more personal data than the kind of information that infection-logging viruses like Marker.A share to their downstream victims. The amount of information shared by employees that use IM clients at work may not be appropriate or acceptable to their employers.

When employees use IM clients to send and receive files, and share a directory of files, they allow third parties to view the IP address of their computers. This only makes it easier for hackers looking for a way in. The following is the disclaimer AOL's ICQ client shows to users when the Share Files feature is enabled:

> "Please note that as in any remote access program, by activating the Shared Files feature and allowing third parties remote access to certain files on your computer, you increase the risk that someone will tamper with your computer. Furthermore, note that by activating the Shared Files feature, you enable third parties to view your IP address."

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

AIM's license agreements states:

> "... In sending and receiving files, other Service users may also be able to determine your IP address ..."

The next, and possibly most serious, privacy issue is loss of confidential information. This can happen a number of ways. As stated above in AOL's ICQ Shared Files feature agreement, you have no way of knowing who will have access to the files you place in the ICQ file sharing folder. Anything confidential placed there will be exposed to everyone on the Internet. Also, a disgruntled employee could easily send files, or confidential IM text messages, to a competitor. If they were afraid of employer monitoring of IM traffic, they could also cloak the information using stegonography utilities to hide the contents of transferred files.

Most people that use IM clients in the workplace are completely unaware that every message they send – even to a co-worker sitting in the next cubicle – has to pass through the company firewall to the service provider's servers and get relayed back through the firewall to end up on their co-worker's desktop. All of the messages sent back and forth by users travel across your network and the Internet in plaintext and can easily be captured and read using a simple network monitoring program (Berg, p.46). In other words, even if two co-workers have no intention of sharing information with the entire world and think they're engaged in a confidential IM discussion at work, they may have the attention of an interested third party. For IM clients to be acceptable in an enterprise environment they would have to include automatic encryption of all messages.

Identity Issues

Anyone can impersonate anyone else on the Internet. There's no way of knowing that the person you're communicating with is really who they say they are when using a free IM service. Even if you know someone's "screen name", you still can't be certain that the person using it is who they say they are. It's trivially easy to get someone's password by using a keyboard logger or reading the registry (Berg, p.46). Most advanced remote access Trojan horse clients like Netbus and Subseven include both abilities. There are plenty of Trojans that are designed solely to steal passwords (online identities) as well. For IM clients to be acceptable in an enterprise environment they would have to provide strong authentication.

Malware in Transferred Files

Any of the free IM clients that allow file transfers could allow infected files to bypass conventional antivirus protection. Most companies protect all messages passing through their e-mail servers, but like free Internet e-mail services (Hotmail, Yahoo!, etc.), IM file transfers bypass antivirus protection efforts in most cases. Gateway antivirus products may help, but they would need to be installed either on a proxy server or on a firewall server. Many companies aren't willing to take the performance hit that either solution would produce, and it's unlikely that any antivirus product can keep up with all traffic on a busy gateway anyway.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The best defense then is to have reliable desktop antivirus protection and frequent automatic signature updates. Yahoo! Messenger 5.0 allows users to specify an antivirus program to scan all files that a user receives. But as long as the computer has a real time antivirus program running, and its virus signatures are kept up-to-date, IM antivirus plug-ins shouldn't be necessary.

Not only can malware come in through transferred IM files, naive users may be convinced by an attacker to install a booby trapped IM client that either does damage to the victim's computer, or installs a Trojan horse backdoor that allows access to the victim's computer (Berg, p.42).

Client Security Bugs

There has been a lot of press coverage lately concerning the security holes found in both of AOL's IM clients. First, an overflow was discovered in the AIM 4.7 and 4.8 (Beta) code that parses game requests by w00w00 Security Development. According to Matt Conover, the author of the w00w00 security advisory that was released to the Bugtraq and NTBugtraq mailing lists, the vulnerability would allow remote penetration of the victim's system without any indication as to who performed the attack and that there would be no opportunity to refuse the request (Conover). Unfortunately, Conover also included most of the code necessary to create an exploit, and the workaround AIM Filter program recommended in the advisory contained a spyware application. w00w00 released the exploit code because AOL never responded to their contact attempts, according to Conover. AOL responded very quickly after the exploit code was made public, however. The bug was fixed on AOL's servers the next day. Users didn't need to download a patch for their clients.

Next, a similar bug was found in AOL's ICQ client in the voice, video and games feature request. No exploit code was made public, but the solution to the ICQ bug requires a client upgrade to the latest build of version 2001b, #3659. Earlier builds of version 2001b are vulnerable, but not to direct connection requests unless the user configured their client to accept direct connections from anyone, which isn't the default setting. According to CERT Advisory CA-2002-02, an exploit exists, but they don't think it's been distributed in the wild. They have not seen active scanning for the vulnerability, nor have they received any reports of this vulnerability being exploited (Rufail).

The CERT Advisory also stated the following:

> "Some versions of the ICQ client open port 4000/UDP for client-server communication. Other versions open port 5190/TCP for this communication. As with the previously reported AIM vulnerability, AOL has modified the ICQ server infrastructure to filter malicious messages that attempt to exploit this vulnerability, preventing it from being exploited through an AOL ICQ server. Exploiting the vulnerability through other means (man-in-the-middle attacks, third-party ICQ servers, DNS spoofing, network sniffing, etc.) may still be possible. Also, since UDP packets can be broadcast on a network, a malicious TLV packet with a spoofed source IP address may be accepted as a legitimate server message.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Given that the Nimda.A worm, which made use of fairly old vulnerabilities in Internet Explorer and IIS 4 and 5 installations that hadn't been patched, was able to infect over 500,000 Microsoft IIS servers, I'm not sure casual ICQ users could be expected to understand the gravity of the problem, or necessarily be expected to upgrade their software. Not to mention that most of the press releases failed to mention that earlier builds of ICQ version 2001b are still vulnerable and many users may think they're not in danger. Most likely, many vulnerable clients will remain unpatched, especially since AOL reports 122 million users of ICQ.

A more reliable means of keeping IM clients relatively secure, at least for home users anyhow, would be through automatic updates of the software. Hackers will continue their efforts to find holes in messaging clients because of the built-in roadmaps to other users that can be exploited – the contact or "buddy" lists. That, and the ability to for an attack to spread around the Internet within minutes are strong motivators to malware authors (Reuters). Self-updating clients would put the responsibility for security patches solely on the software vendor and out of the end users' hands, although they could also update the software with even worse holes.

Less serious buffer overflow security bugs have been found in all four top IM clients, and will probably be found again in the future. The w00w00 advisory stated that "An exploit could easily be amended to download itself off the web, determine the buddies of the victim, and attack them also." (Conover). Tony Lambiris, who wrote an exploit called AIMrape that could cause a Denial of Service (DoS) on any Windows AIM user's computer, wrote that "To have an e-mail attack be successful, you need to send it, have the party download it, save the attachment, and run it. With a messaging system, all you need to know is the person's user name." (Reuters). Incidentally, Lambiris' exploit made use of a known buffer overflow in AIM. AOL patched the bug a week after the exploit was made public.

Carey Nachenberg, chief architect for anti-virus firm Symantec Corp.'s security response team, put it this way: "Imagine a day when all these people are on with broadband connections – they are always connected, their computers are always on, and a computer worm targeting a popular messaging system starts spreading. That would potentially ravage hundreds of millions of machines." (Reuters). Luckily, that hasn't happened yet. So far, all found vulnerabilities have been reported to the vendors so the software could be patched. Someday a less responsible hacker may find another IM client buffer overflow that allows code of the attacker's choice to be run on the victim's computer and exploit it as a worm.

Another, less obvious vulnerability that could theoretically effect AIM and MSN Messenger, due to their use of ad banners, is the slight chance that someone may be able to hijack the ad banner server and replace the banners with their own. The replacement banners could range from just annoying and embarrassing jabs at either service vendor, to the far worse case where they could contain something like an intentionally corrupted Flash SWF file that might possibly cause a DoS for every user of the service (Krawetz). Either way, it would cause a huge loss of user confidence and loyalty for the service.

Solutions

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Based on what we've seen, it would be hard for any business to make a case for installing a consumer grade IM client in the workplace. The security threats are just too great, and besides, the clients aren't compatible with one-another. But IM will undoubtedly be coming to an enterprise near you, and probably before the end of the year. So, from a security perspective, the best course of action is to establish, distribute and enforce written security policies concerning the use of consumer grade IM clients in the enterprise, make sure antivirus protection is in place and functioning properly on servers, gateways and desktops, determine the need for alternative, secure IM solutions, and tighten up the firewall to prevent any rogue users from connecting to outside IM services (Berg, p.49). Software auditing and IM monitoring may also be necessary to enforce the security policy.

Establish, Distribute and Enforce Written Security Policies

If your company doesn't have an established written security policy, one will have to be created that takes into account all possible security issues that can be identified and defined. A good place to start when creating security policies is the SANS Security Policy Project whose "goal … is to offer everything you need for rapid development and implementation of information security policies". It's located at http://www.sans.org/newlook/resources/policies/policies.htm. The Security Policy needs to clearly state accepted company policies, necessary actions, and responsibilities. It also needs to be signed by someone with sufficient authority and credibility that it is accepted by the members of the organization to which it applies (Estep, p.6). Policies address what is to be done, who is to do it, and why (Estep, p.23).

If your company already has an existing security policy, review it and update it to include coverage for free IM clients and other Peer to Peer (P2P) applications (file sharing applications like Napster and Gnutella and distributed processing applications like Distributed.net or SETI@Home clients). Policy regarding these issue-specific problems would likely be written as sub-documents to the main corporate security policy.

Once your security policies have been either created or updated, make sure they're distributed to all employees. You may want to have the Payroll department hand out copies to all employees with the paychecks to make sure they're distributed. Requiring employees to sign an acknowledgment form that states that they've read and understand the company's security policy is also an option. Although it can, and should, be posted on the company's Intranet or other readily accessible public location on the network, just putting it there and saying "come and get it" isn't sufficient, but it's much better than taking the time to create a security policy and then keeping it in an obscure, or inaccessible location. It is required reading for all employees and should be included in the employee handbook.

Responsibility for enforcement of the security policy should be established in the policies. Enforcement can be helped by software auditing products that will identify where the clients are installed like FaceTime's IM Auditor, and by IM monitoring software like the solutions produced by SurfControl, WebSense and Elron. A company called eSniff also makes a hardware device that monitors IM use. If Windows 2000 and Active Directory are in place, users could be restricted from installing unapproved software through Group Policy. Otherwise, Desktop

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Management tools could be used to treat IM clients as licensed applications with no licenses available to prevent their installation.

Ensure Antivirus Protection is in Place and Functioning

Due to the threats caused by IM clients, and their ability to bypass security, make certain you have antivirus protection installed on your servers, gateways and desktops. Multi-layer protection is essential to effectively keep infections at bay. Choose a utility that's fast and accurate for real-time and scheduled scanning of your servers. Gateway antivirus products should also be chosen that are relatively non-intrusive and cause the least detriment to performance. They should also be able to keep up with a high amount of traffic laden with large numbers of attachments as well as possible. They could also be used in conjunction with a policy-based content inspection utility like MIMEsweeper (formerly owned by Baltimore Technologies). And desktop protection should be chosen that would cover all the bases, from malicious ActiveX and Java applets to HTML based e-mail worms like KAK.A. Since desktop antivirus utilities are the last line of defense, its implementation should be considered carefully.

It's best to use a different vendor for each area of protection to increase your chances of stopping virus infections or malware. Use of different products with different engines, signatures, and heuristic pattern recognition is essential even in the smallest of networking environments. Different products produce different false positives, so using different vendors helps in determining when identifications are correct if they're thought to be suspicious. Online virus scanners from nearly any one of the antivirus vendors, like Trend Micro's HouseCall, can help in that respect, too. Vendors are able to update their signatures at different regular schedules as well, and the speed at which viruses are included in signature updates fluctuates. While a vendor may be quick with including one hot virus and beat all of their competition with a signature update one time, they may not be so expedient with the next one to come along. Also, vendors occasionally release bad signatures with lots of false positives, or that cause other, much worse problems like locking up computers completely. Using multiple vendors keeps you from putting all your eggs in one basket, so to speak.

Different vendors include different types of programs in their signature files as well. Some vendors include games and annoying harmless pranks in addition to serious threats in their signature definitions. Some include "hacker utilities" which are very useful for network security analysis. Be sure to choose vendors whose signature definitions are compatible with your needs.

Also make sure that the signatures are updated as often as possible – preferably automatically every three to four hours. Twenty four hours is about the longest you would want to go without checking for new signatures for any platform's protection. Unfortunately, that may be the most frequent setting you can choose for some products. If that's the case, you may be able to script manual command-line updates that can be scheduled more frequently using the Windows Task Scheduler, depending on the antivirus software package. Also, if possible, set up distribution servers for scheduled client updates (more than one for load balancing) to reduce Internet bandwidth use. The signatures will install much faster from servers on your network.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

An emerging technology called behavior-blocking may also be worth looking into as a supplement to traditional antivirus software, but not as a replacement. Behavior-blocking software runs on server and desktop computers, and is instructed through policies that network administrators set to let benign actions take place but to intercede when unauthorized actions occur (Messmer). Behavior-blocking software "sandboxes" suspicious code till it can be examined. Products are available from Okena, Entercept, Pelican Security, Aladdin Knowledge Systems, Finjan, Granite Technology, Sandbox Security, Secure4You and Harris. No traditional antivirus software companies have shown interest in the technology yet.

A very good source of information on available antivirus products is the University of Hamburg Computer Science Department's Virus Test Center (VTC) at http://agn-www.informatik.uni-hamburg.de/vtc/eng1.htm. Although the information isn't necessarily up-to-date, their testing is extremely thorough. Unfortunately, a few vendors refuse to allow their products to be tested due to unfavorable past results.

Determine the Need for Alternative Secure Instant Messaging Solutions

The argument in favor of instant messaging as a productivity booster in the workplace points out the ability to see when other users are available to help avoid the downfalls of phone and e-mail conversations. IM doesn't have the inherent delays that the other two means of business communication do; there are no missed calls or lengthy waits for replies. And IM clients allow more collaboration in the form of chat services. But it just isn't secure enough to use in the workplace.

If, after stopping your users from using consumer IM clients, you determine the need for an immediate solution, before the technology has a chance to develop into robust, secure real-time collaborative applications, there are plenty of alternatives. For internal use, there's Lotus' SameTime for Lotus Notes collaboration, Groove Network's Groove which has shared file update distribution, Parlano's which has chat rooms secured by encryption (Berg, P.46), UBS Warburg's MindAlign which features archiving of messages (George and Swanson), Microsoft's MSN Messenger and Windows Messenger clients for use with Exchange 2000 and the Exchange Instant Messaging Service, JabCast's Secure Realtime Communications (based on open-source Jabber), and Java-based NetLert and Bantu that both make use of SSL. External, secure services include United Messaging's Enterprise Instant Messaging. And IM services developed for use in call centers include FaceTime Communications' IMAuditor that works with AOL, MSN, and Yahoo! IM clients and services (George and Swanson), Tribal Voice PowWow service that also works with AOL, MSN and Yahoo! services, and LivePerson which uses SSL encryption for chatting with clients.

Tighten up the Firewall

Tightening up the firewall is probably the least effective means of preventing customer grade IM client use in the workplace. Even if you only allow traffic through port 80 (HTML), IM clients will use it if they have to (Berg, p.50). But they do need to connect to host servers so blocking access to them is somewhat effective if you can block all IP addresses associated with the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

services' host servers. That may prove to be a bit of a chore since the addresses associated with the different services' hosts may change from time to time.

To block AOL's AIM you need to block traffic to login.oscar.aol.com, which points to the following IP addresses, according to a DNS lookup (Berg, p.51):

205.188.7.172
205.188.7.176
205.188.7.164
205.188.7.168

Similarly, to block Yahoo! Messenger you need to block access to the hosts that answer to the following names, each resolving to multiple IP addresses (Berg, p.51):

msg.edit.yahoo.com
edit.messenger.yahoo.com
csa.yahoo.com
csb.yahoo.com
csc.yahoo.com

MSN Messenger use can be stopped by blocking access to the Hotmail network range – 64.4.0.0 through 64.4.63.255 (Berg, p.51).

Conclusion

Consumer grade instant messaging client use in the enterprise is growing fast and its use oftentimes goes unchecked. The use of these free applications in the workplace creates a serious threat to security due to privacy issues, identity issues, malware in transferred files, and client security bugs. The best way to stop the trend of unwanted and unchecked installation of instant messaging clients by employees is to establish, distribute and enforce written security policies, make sure antivirus protection is installed and frequently updated on gateways, servers and desktops, determine the need for secure alternatives, and tighten up the firewall to block access to the free instant messaging services' public hosts. With this course of action, the enterprise should be safe from the instant messaging menace.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Bibliography

1. Gartner, Inc. May 1, 2001 Press Release. May 1, 2001.
URL: http://www.gartner.com/5_about/press_room/pr20010501b.html.

2. Gartner, Inc. October 11, 2001 Press Release. October 11, 2001.
URL: http://www4.gartner.com/5_about/press_releases/2001/pr20011011a.html.

3. Berg, Al. "P2P or Not P2P?" Information Security. February 2001: 38-51.

4. Langa, Fred. "Langa Letter: More Instant-Messaging Security Holes." InformationWeek. Oct 1, 2001 (12:00 AM).
URL: http://www.informationweek.com/story/IWK20010927S0021.

5. Ryan, Michael E.. "Don't Kill the Instant Messenger." PC Magazine. December 26, 2001: 36, 40.

6. George, Tichelle and Swanson, Sandra. "Not just Kid Stuff." InformationWeek. September 3, 2001 (12:00 AM).
URL: http://www.informationweek.com/story/IWK20010830S0030.

7. Conover, Matt. "AOL Instant Messenger Overflow." w00w00 Security Development Advisory. January 2, 2002.
URL: http://www.w00w00.org/advisories/aim.html.

8. Reuters. "Instant Messaging: Open Door for Hackers?" December 3, 2001.
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2829503,00.html.

9. Krawetz, Neal. "Flash and Crash – Security Vulnerabilities in SWF Files." SecuriTeam. January 28, 2001.
URL: http://www.securiteam.com/securitynews/5PP110035W.html.

10. Marsan, Carolyn Duffy. "Threat to 'Net." Network World. January 14, 2002.
URL: http://www.nwfusion.com/news/2002/0114instantmessaging.html.

11. Rafail, Jason A. "CERT® Advisory CA-2002-02 Buffer Overflow in AOL ICQ." CERT/CC. January 24, 2002.
URL: http://www.cert.org/advisories/CA-2002-02.html.

12. Messmer, Ellen. "Behavior Blocking Repels New Viruses." NetworkWorldFusion News. January 28, 2002.
URL: http://nwfusion.com/news/2002/0128antivirus.html.

13. Estep, Brian M., Kolde, J., and Wendt, Carla. "Basic Security Policy." Track 1 – SANS Security Essentials 1.2 SANS Security II: Network Security. The SANS Institute, 2001. Section 2, pages 1 - 40.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced