Jennifer Sanders

Security Management: Instant Messaging Perspective

Executive Summary

Nowadays, Instant messaging (IM) is used in the corporate environment which is rising rapidly, as organizations welcome to accept IM as a business communications tool. IM promotes cooperation and real-time communication among employees, business partners, and customers. It also brings new threats to local area network security and makes organizations to have a potential risks when employees share illegal or inappropriate content over the internet.

Organizations are also faced with reduced employee productivity when IM is used arbitrarily and for personal communications. When use of IM is unmonitored and uncontrolled, it can lead to a significant drain on IT resources, as the IT staff attempt to identify which IM applications are being used and by whom. Moreover, when instant messaging is used to send and receive files, not only can the resulting drain on bandwidth negatively impact network performance, but the files themselves can pose a serious security threat.

This report provides information to better understand threats of IM and mitigate its impact to business. The threats of IM are investigated. The trend in growing targets and number of cases are related to IM threats are analyzed. The impacts to business are assessed to identify areas of security management require great concern. Finally, measures are introduced to improve security management such that IM threats become manageable and their impact is reduced.

1. Introduction

Today, Instant Messaging (IM) applications have rapidly become accepted by businesses as viable employee communications tools. IM is more instant than email, obviously easy-to-use, and provides the real-time collaboration organizations need to ensure quick judgments and decisions.

Using Instant Messaging, organizations and their business partners can make a conference, share files and information easily over the Internet. Furthermore, within the organization, IM conversations among project team members can resolve issues and questions in an instantsomething that might have taken a series of emails, telephone calls, or face-to-face meetings to carry out. IM can be used to provide immediate replies to requests. It can also help promote personal relationships with customers and remote employees, and assist customers in completing transactions with Web-based businesses. This report is shown the concern of security of IM and gives some countermeasure to deal with IM threats.

2. Findings and Analysis

2.1 What threats are related to Instant Messaging?

l Worms

A worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes and it may do without any user participation. In case of instant messaging, antivirus software does not currently monitor traffic at OSI Model-network layer. If a worm starts to spread via instant messaging, it cannot be stopped before it reached the remote's computer. Dissimilar a virus, it does not need to attach itself to an existing application or program. Worm almost always causes damage to the network when it drains the network bandwidth. On the contrary, virus almost always corrupt or modify files on a targeted computer.

The number of instant messaging worms is rising steadily. This is made clear when one considers the list of recent IM worms:

n dubbed Pykse.A (16 April 2007)

n W32/Rbot-GRS (26 June 2007)

However, a few antivirus applications can plug in to instant messaging clients for scanning files when they are received. The lack of applications scanning instant messaging network traffic is partly due to the difficulty in monitoring instant messaging traffic so that the antivirus product running at the desktop level can catch the worms.

l Backdoor Trojan Horses

Instant messaging clients allow peer-to-peer file sharing, the instant messaging client to share all files on the system with full access to everyone can be configured by a Trojan Horse and in this way gain backdoor access to the computer. Moreover, the victim computer is on-line; a notification will be send to hacker automatically. So hacker can keeps track and accesses the infected computer easily. Besides, the hacker does not need to open new suspicious ports for communication in that hacker can instead use already open instant messaging ports.

Classic backdoor trojans open an outgoing listening port on the computer, forming a connection with a remote machine. If the trojan operates via the instant messaging client, it does not open a new port as the user has usually already created an allow rule for instant messaging traffic to be outbound from their machine, therefore, allowing the backdoor trojan horse using the same channel to go unblocked.

l Hijacking and Impersonation

Users can be impersonated in many different ways by hacker. The most frequently used attack is solely stealing the account information of an unsuspecting user using the instant messaging or IRC application.

Hacker can execute a password-stealing trojan horse to obtain the account information of a user. If the password for the instant messaging client is saved on the computer, the hacker could send a trojan to an unsuspecting user. When trojan executed, it would find the password for the instant messaging account used by the victim and send it back to the hacker.

l Denial of Service

Instant messaging may lead a computer vulnerable to denial of service (DoS) attacks. These attacks may have different outcomes: A lot of DoS attacks make the instant messaging client crash, hang, and in some cases consume a large amount of computer processing power and causing the entire computer to become unstable.

There are many ways in which a hacker can cause a denial of service on an instant messenger client. Furthermore, they are used to combine with other attacks, such as the hijacking of a connection and form a bot network to attack other servers.

l Unauthorized Disclosure of Information

Information disclosure could occur without the use of a trojan horse. Once the data that is being transmitted via the instant messaging network is not encrypted, a network sniffer can sniff data on most types of networks and can be used to capture the instant messaging traffic. Also, a hacker could sniff the packets from an entire instant messaging session. It can be very dangerous as hacker may gain access to privileged information. It is especially dangerous in the corporate environment in that confidential information may be transmitted along the instant messaging network.

2.2 Recent Incidents

Case 1: New IM worm targets Skype users (Published date: 17 Apr 2007)

Affected: The IM worm affects Skype users running Windows.

Threat Type: Worm

Description: 'A new instant-messaging pest that spreads using the chat feature in Skype has surfaced, security firm F-Secure warned. The worm, dubbed Pykse.A, is similar to threats that affect instant-messaging applications. A targeted Skype user will receive a chat message with text and a Web link that looks like it goes to a JPEG file on a Web site, F-Secure said on its Web site. Clicking the link will redirect the user to a malicious file. The file, after executing, will send a malicious link to all online contacts in a Skype user's list and will show a picture of a scantily clad woman, F-Secure said. In addition, it sets the user's Skype status message to "Do Not Disturb," the security firm said. Pykse also visits a number of Web sites that don't host any malicious code and a site that appears to count infected machines, F-Secure said. The Finnish security company doesn't list any particular malicious payload for Pykse other than it spreading and visiting Web sites.'

Status: Skype also recommends using antivirus software to check the files received from other people.

Case 2: Next-generation Skype Trojan hits web (Published date: 26 Mar 2007)

Affected: Warezov Trojan horse to target Skype users.

Threat Type: Trojan Horse

Description: 'Miscreants have again adapted the Warezov Trojan horse to target Skype users. The attack is similar to threats that target instant-messaging applications. A targeted Skype user will receive a chat message with the text "Check up this" and a link to a malicious executable called file_01.exe on a website. Once infected, a computer will be at the beck and call of the attacker and the Trojan horse will start sending messages to the victim's Skype contacts to propagate.'

Status: Skype warned users against opening the malicious file, take caution in general when opening attachments, and also recommends using antivirus software to check incoming files.

Case 3: AIM bot creates "fight combos" to spread (Published date: 18 Sep 2006)

Affected: Online attackers have created an instant-messaging bot program for AOL instant messaging that chains together a number of executable files, similar to the combination moves in fight games.

Threat type: Worm and Bot

Description: 'The software, dubbed the AIM Pipeline worm, uses modular executable files to infect machines with different functionality but also to make the bot network's growth more robust: if a Web site hosting one of the components gets shutdown, the other pieces of the worm can still spread.'

Status: America Online has blocked the URLs used in the messages sent by the AIM Pipeline worm.

2.3 Trends

l Increase in IM threats

'IM Security Center researchers tracked 33 malicious code attacks over IM networks during the month of September, bringing the 2007 total to 297. This is a 20% increase in IM threats compared with the same time period last year.' (SAN DIEGO -- Akonix Systems, Inc 2007)

'Research also indicates that there are more targets affected by IM threats' (SANS Institute 2006)

l New type of IM worms

'New IM worms identified include Agent-GCG, Ataxbot, Exploit-VcardGadget, Focelto, MSNFunny, IMBot, MsnSend, MSN-WhoBlocked, Neeris, Pykse, Skipi, STRATION and Yalove. IRCBot was the most common with four variants, followed by Imaut and Neeris with two, respectively. Akonix tracked 16 attacks on P2P networks, such as Kazaa and eDonkey' (SAN DIEGO -- Akonix Systems, Inc)

l Evolution of IM threats

The vulnerability of IM are used in botnet communication and spread the bot and worms to another computers. When the hacker send the command to botnet army, the consequence of attacks is very serious. Unlike other attacks, botnet can comprised of thousands of computer power to perform a variety of attacks against a wide range target. For example, the botmaster can command each zombie participant in a botnet to launch spamming e-mails to steal the credit card information and launch Distributed Denial-of-Service (DDoS) attacks simultaneously against the thousands of computer.

2.4 Factors for growth of IM threats

The growth of instant messaging usage within the organization, vulnerabilities in public IM networks occur during the process of transferring files. When a user transfers files or uses other IM features like file sharing or voice chat, user's IP address is revealed. Using this IP address, hackers can have ability to attack the system. Some organizations configure their firewalls to block ports used by IM applications or block the external addresses of IM network servers. But IM applications can be configured to change ports automatically and are capable of penetrating firewalls through ports used by other applications. (For example: port 80). So policy control management is required.

3. Impact to Business

Once the IM threats occur in the organizations, they face a significant security risk from disclosure of intellectual property or business-critical information using IM's file attachment capability. As IM is a highly informal means of communication, employees can unintentionally send critical company-confidential information, such as product specifications, code, and blueprints, or private customer data, to friends, colleagues, and competitors. There are three main concerns of using the IM which are identified.

l Legal Liability concerns

The danger of allowing employees to use IM at work under lacking of security management, the viruses and worms is very easy to expose. On the other hand, organizations face legal and compliance risks when employees share copyrighted, illegal, or inappropriate content via instant messaging. Unmonitored IM applications allow employees to openly transfer files and information that could lead to significant corporate liability. For example, transferring copyrighted MP3 files, movies, and software using IM is common among friends and bypasses the file size restrictions of email.

l Employee productivity loss

Many employees have already adopted IM which they prefer that IM is regarded as the personal connection with friends of family, because it has not used the telephone to be obvious, talking can't be eavesdropped. Employees can seem it is work, in their keyboard is typed and left, been exchanging the personal connection with friends of family all the time.

l IT resource abuse

Most organizations don't know what kind of IM should be installed on computer, which employees should use the IM and how often to use IM for business communication such as send, receive files, video conferencing. In addition, it is not uncommon for intensive file sharing over the IM that can influence the performance of the network.

4. Dealing with Instant Messaging threats

IM threats can be operated by insider (employees) and outsider (hacker). According to the Figure 4-1, Operational-level employees want to increase their ability to override controls mechanisms base on some factors such as fear of lose their job whereas the top level-manger want to have control mechanism to monitor all harmful activity in the organization. However, top level-mangers always neglect the risk of middle-level managers whose have part of administrative power to act as insider. So that good security management must be executed in the organization to avoid or mitigate the insider and outsider activities. Consequently, prevention, detection, incident response and controls are good measures for security management.

4.1 Prevention

n Ensure that vendor patches are promptly applied to instant messaging software, interrelated applications, and the underlying operating system.

n Firewalls to separate all DMZs, internal networks and external un-trusted networks

n Monitor using an Intrusion Detection/ Prevention system for users.

n Create secure communications channel when using instant messaging with trusted business partners

n Do not rely on external IM servers for internal use of instant messaging.

n Install and use anti-virus and anti-spyware applications.

n Consider disposing the clear products designed for instant messaging safely.

n Some product like as Trend Micro IM Security for Microsoft Office and Symantec IM Manager 2007 seamlessly manages can be used for mitigation of the potential risks associated in that they acts a filter and detector between internal and external.

n Using Multi-factors authentication or biometric authentication to prevent the hacker to login the target computers.

4.2 Detection

n Monitor and detect using an Intrusion Detection for users creating tunnels for instant messaging. An intrusion detection system (IDS) generally detects unwanted manipulations of computer systems, mainly through the Internet.

n Enable the auto detect mode of updated antivirus and anti-spyware products for client computer.

n Filter all http traffic through an authenticating proxy server or firewall to provide additional capabilities of filtering or monitoring instant messaging traffic.

n Appropriately configure intrusion detection systems. Understand that many instant messaging applications are capable of enabling associated communications to masquerade as otherwise allowed traffic (e.g. http).

4.3 Incident Response

n Block popular instant messaging ports.

n Block access to known public instant messaging servers that have not been explicitly authorized.

n Virus-scanning software at all critical entry points such as firewalls, remote access server, e-mail servers etc.

n Ensure that vendor patches are promptly applied to instant messaging software, interrelated applications, and the underlying operating system.

4.4 Management & Policy Controls

n Establish policies for acceptable use of instant messaging and ensure that all users are aware of those policies and clearly understand the potential risks.

n General users should not be allowed to install software. Limit Administrative and Power User level privileges to support personnel with their support ability. If a user must have Administrative or Power User privileges, create a separate account to be used for their daily office functions, internet surfing and on-line communication.

5. Conclusion

Instant messaging has clearly taken off as a means of communication. The ability to communicate in real-time makes it an ideal medium for both business and personal communication. Unfortunately, threats that affect instant messaging already exist today, including worms and vulnerabilities that can give hackers remote access to vulnerable computers and can replicate in seconds can affect more than just instant messaging.

Therefore, end users and corporations should employ basic security countermeasure.

However, update the patch of product can mitigate the occurrence of threats, but these measures are not enough to prevent the network security. Corporations should have other measures for security such as prevention, detection and incident response. Furthermore, management controls are available to less the impact of IM threats. Once these measures get implement, IM threats must become manageable as a result of reducing the damage of business.

Reference

1. Michael E. Whitman and Herbert J. Mattord (2004) *Management of Information Security*, Boston, Mass.; London: Thomson/Course Technology

2. Joris Evers (2007) New IM worm targets Skype users, *Cnet*, Available: http://www.zdnet.com.au/news/security/soa/New-IM-worm-targets-Skype-users/0,130061744,339274904,00.htm (17 Apr 2007)

3. Joris Evers (2007) Next-generation Skype Trojan hits web*, Silicon*, Available: http://software.silicon.com/malware/0,3800003100,39166534,00.htm (26 Mar 2007)

4. (2006) AIM bot creates "fight combos" to spread, *Security Focus*, Available: http://www.securityfocus.com/brief/305 (18 Sep 2006)

5. San Diego (2007) Akonix Intros IM Security Appliance, *Dark Reading*, Available: http://www.darkreading.com/document.asp?doc_id=125041&WT.svl=wire_2

(29 MAY, 2007)

6. San Diego (2007) Akonix's Threat Center tracks 33 IM attacks , *Dark Reading*, Available: http://www.darkreading.com/document.asp?doc_id=135045

(28 Sep 2007)

7. SANS Institute (2006) *SANS Top-20 Internet Security Attack Targets*, Available: http://www.sans.org/top20/ (15 Nov 2006)

8. Symantec (2006) *Protect Your Business from Instant Messaging Threats*,
Available:
http://www.symantec.com/business/library/article.jsp?aid=instant_messaging_threats
(11 Jul 2006)

9. Symantec (2007) *Internet Security Threat Report 2007*,

Avalable: http://tc.imlogic.com/threatcenterportal/pubIframe.aspx (13 Jun 2007)

Word Count: 2750