Threats to Instant Messaging

By Neal Hindocha
Symantec Security Response

INSIDE

› Threats to Instant Messaging
› Blocking Instant Messengers
› Summary
Contents

Introduction ................................................................. 3
Background ................................................................. 3
   AOL Instant messenger (AIM) ........................................ 3
   ICQ (“I SEEK YOU”) .................................................. 8
   Yahoo! Messenger .................................................... 9
   MSN Messenger (also known as Windows Messenger) ........... 11
Threats to Instant Messaging ........................................... 13
   Worms ................................................................. 13
   Backdoor Trojan Horses ............................................. 14
   Hijacking and Impersonation ....................................... 15
   Denial of Service ..................................................... 16
   Information Disclosure ............................................. 16
   Threats Specific to AIM ............................................. 17
   Threats Specific to Yahoo Messenger ............................. 19
   Threats Specific to ICQ .............................................. 19
   Threats Specific to MSN Messenger ............................... 20
Blocking Instant Messengers .......................................... 21
The Future of Instant Messaging ..................................... 22
Summary ........................................................................ 22
Introduction

Instant messaging is an up and coming threat as a carrier for malware. More and more people are using instant messaging, both for personal and business reasons. Instant messaging networks provide the ability to not only transfer text messages, but also transfer files. Consequently, instant messengers can transfer worms and other malware. Instant messaging can also provide an access point for backdoor Trojan horses. Hackers can use instant messaging to gain backdoor access to computers without opening a listening port, effectively bypassing desktop and perimeter firewall implementations. Furthermore, finding victims doesn’t require scanning unknown IP addresses, but rather simply selecting from an updated directory of buddy lists. As more functionality is added to instant messaging, such as peer-to-peer file sharing, instant messaging will also become more prone to carrying malware.

Furthermore, instant messaging is very difficult to block in a company using conventional security methods such as firewalls. In addition, there are generally no antivirus applications monitoring instant messaging network communications on the server level. This means an instant messaging worm can be caught only at the desktop level.

Fortunately, antivirus vendors have realized the dangers of instant messaging, and have begun to create plug-ins for the various instant messaging clients in their desktop products. Norton AntiVirus 2003 is an example of an antivirus product that will plug in to the various clients and scan any incoming files.

When email became a part of our daily lives, it also became a large carrier of worms. Even after many email worm outbreaks, people are still not educated about the potential dangers of email usage. Hopefully, the same story will not be repeated with instant messengers.

Background

This paper will concentrate on the four most popular instant messaging networks and their default clients. This includes AOL Instant Messenger (AIM), ICQ, MSN Messenger (also known as Windows Messenger), and Yahoo! Messenger. Many other third-party clients have been written to interact on these networks that may be affected in a similar manner by worms and exploits; however, these will not be discussed directly.

The protocols for these instant messaging networks have been reverse-engineered or released by the vendor. AOL owns both AIM and ICQ, and the later versions of the ICQ client use a protocol very similar to the AIM protocol. MSN Messenger belongs to Microsoft, and Yahoo! Messenger is created and distributed by Yahoo!

The idea of utilizing instant messaging for malicious purposes is not simply theoretical. In fact today, there are over 20 different worms that use instant messaging to spread, many of which have been fairly widespread. W32Choke.Worm is an example of a prevalent worm that spreads using MSN Messenger.
AOL INSTANT MESSENGER (AIM)

The AIM client. The client is free, and can be downloaded from http://www.aim.com.

Protocol

The AIM service can use two different protocols. The protocols are called OSCAR and TOC.

OSCAR is considered to be the main protocol for accessing the AIM service. It is a binary protocol, and it is the protocol that is used by the AIM client. AOL has not released the specifications of the OSCAR protocol. Furthermore, AOL has attempted to block third-party clients that use the OSCAR protocol. An example of a client that AOL attempted to block is Trillian (http://www.trillian.cc).

TOC is the second protocol that can be used to access the AIM service. TOC was developed so third-party vendors could write their own clients, and to help the development of clients under non-Windows operating systems such as Linux. AOL makes the specifications for TOC publicly available. However, the TOC protocol is less functional than OSCAR.

TOC does not allow any functionality other than chatting. Furthermore, it restricts the maximum packet-size to 1024 bytes, which means single messages sometimes need to be split up into several packets.

In this paper, only the OSCAR protocol will be discussed. Therefore, any reference to an AIM protocol is a reference to the OSCAR protocol.
Data Packets

Documentation regarding the AIM protocol can be found easily on the Internet allowing one to write a compliant client and/or a server. However, the documentation is not complete and AOL has since updated the protocol. Nevertheless, reverse-engineering the protocol is relatively easy by monitoring the AIM network traffic since the AIM packets are not encrypted in any way.

AIM communicates over TCP using a proprietary AIM protocol. One TCP packet can contain more than one command, and one command can require more than one TCP packet.

The AIM protocol is called OSCAR, and the normal packets are called FLAP. Most of the commands are sent in SNAC packets that are contained within the FLAP packets. Each FLAP packet has a FLAP header.

The header appears as follows:

<table>
<thead>
<tr>
<th>BYTE</th>
<th>Start</th>
<th>0x2A</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYTE</td>
<td>Channel</td>
<td>0x01-0x05</td>
</tr>
<tr>
<td>WORD</td>
<td>Sequence Number</td>
<td>Variable</td>
</tr>
<tr>
<td>WORD</td>
<td>Data</td>
<td>Size</td>
</tr>
</tbody>
</table>

Channel

The start byte marks the beginning of a FLAP package. Each package can belong to one of five channels. Each channel represents a different type of information being transmitted.

The following five channels are currently in use:

- 0x01: New connection
- 0x02: SNAC data
- 0x03: Error
- 0x04: Close connection
- 0x05: Purpose unknown (and very rarely used)

Most communication, such as instant messaging, occurs over channel two.

Sequence Number

The sequence number is initially a random number, which is incremented by one for each FLAP package. The server and the client use different random values. The sequence numbering ensures the reliability of data transmitted and makes hijacking connections or injecting data more difficult without having to parse TCP packets for the TCP sequence number, which serves a similar purpose. If a package arrives and is out of sync to the client, it will disconnect and display an error message. If a package that is out of sync arrives at the server, the server will disconnect the client.
**Data**

The data field holds the size of the data that follows the FLAP header. This data varies depending on the type of transmission.

Data in channel two communications is mostly contained within a SNAC packet.

A SNAC packet header appears as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORD</td>
<td>Family ID</td>
</tr>
<tr>
<td>WORD</td>
<td>Subtype ID</td>
</tr>
<tr>
<td>BYTE</td>
<td>Flag1</td>
</tr>
<tr>
<td>BYTE</td>
<td>Flag2</td>
</tr>
<tr>
<td>DWORD</td>
<td>Request ID</td>
</tr>
</tbody>
</table>

The actual variable sized data follows the header.

**Family ID**

The family ID identifies the packet to which the family belongs.

For example, a packet that tells the server that the client is ready for normal operation would have the family ID 0x0001 (generic control), whereas a packet from the client telling the server that a new buddy is added to the buddylist would belong to family 0x0003 (buddylist management).

**Subtype ID**

Each SNAC packet has a subtype ID as well as a family ID. The subtype further specifies the type of packet.

**Flag 1 & Flag 2**

The purpose of the flags is currently unknown. However, they are not used often.

**Request ID**

This is a pseudo-random number. Whenever the client asks the server for information (or vice-versa), it will add a request ID. When the server responds to the request, it will have the same ID in the request ID field, allowing the client to coordinate request and responses.

**Servers and Ports**

By default, AIM connects to login.oscar.aol.com on port 5190. However, the server and port are configurable, and the server accepts connections on common service ports, such as port 80 (HTTP) and port 23 (Telnet). The AIM client can also attempt to connect to the server by trying a preconfigured list of common ports.

If login.oscar.aol.com is blocked by firewall implementations, AOL provides an http proxy server (www.proxy.aol.com) that can be used to access the AIM service. If an HTTP proxy is used, an HTTP header will be added to all the packets. This will cause the packets to go through even if protocol analysis is being used.
Furthermore, there are many proxy servers available freely on the Internet that can be used to access the AIM service if the entire aol.com site has been blocked.

**Password Encryption**

AIM uses a challenge-response method for sending the password. The server will send a random challenge string to the client. The client will append this challenge string to the password, and then a hash of the password and the appended challenge string is taken. Finally, the hash is sent to the server for verification.

**Login Process**

To connect to the AIM service, the client first connects to the login server, login.oscar.aol.com, and sends the screen name and other associated information.

The server sends a challenge for password verification. The client hashes the password and challenge forming a response and sends back a packet containing the screen name, the password response, and client version information.

After verifying the information, the server sends back a cookie (a random X-bit value) and the IP address of the Basic Oscar Services (BOS) server.

The client disconnects from the login server and connects to the BOS server. It will connect to the same port that was used when connecting to the login server. The client authenticates itself with the BOS server by sending the cookie it received from the login server. The BOS server then sends the client an IP to a services server. This server is used for other services, such as email. If the client does not connect to the services server, an error message will appear on the screen, which can be ignored. The client will function normally even if it is not connected to the services server.

When the client disconnects, the cookie is automatically invalidated. The server also sends a package to the client telling it how often it needs to send keep-alive packets to the server. If this rate is disobeyed, the server will invalidate the cookie and the client will be disconnected.
ICQ ("I SEEK YOU")


ICQ ("I seek you") was originally created by Mirabilis. The first version of ICQ was released in November 1996. The program was very successful very quickly. In June 1997, ICQ handled 100,000 concurrent subscribers.

AOL bought Mirabilis in June 1998. At this point, they had over 12 million registered users.

ICQ does not use buddy names in the same way as AIM, MSN Messenger, or Yahoo! Messenger. Instead, it uses UINs (Unique Identifiers). When a new user signs up for ICQ, a new UIN is created. Therefore, there can be multiple users with the same name, but every ICQ user has a separate UIN.

Protocol

There are several different versions of the ICQ protocol. After AOL purchased Mirabilis, AOL abandoned the original ICQ protocol in favor of their protocol, OSCAR. ICQ uses FLAP packages with only minor differences. The login sequence is identical to AIM, and therefore the password encryption mechanism is also the same.

Servers and Ports

By default, the ICQ client connects to login.icq.com on port 5190. This is the same default port that is used by AIM. Both the default port and server address can be changed.
The ICQ server accepts incoming connections on most standard ports, such as port 80 (HTTP) and port 21 (FTP). Like AIM, proxy servers can be used if direct access to the service is being blocked.

The latest version will automatically detect a blocking firewall and adjust settings as necessary in order to connect to the ICQ server. If direct access to the login server is blocked on all ports, the client will automatically use an HTTP proxy server. If an HTTP proxy is used, the packets will have an HTTP header bypassing protocol analyzing firewalls.

YAHOO! MESSENGER

Yahoo! is a company that was founded in 1994. Yahoo! started as a portal, but today provides many Internet related services.

On June 21st, 1999, Yahoo! released the first version of the Yahoo! Messenger client. The client became popular very quickly, and is now one of the four major instant messaging clients.

Protocol

The Yahoo! protocol is called YMSG. There have been several versions of the protocol, and the current version is nine. Documentation regarding the protocol is available on the Internet, but it is not as well documented as the AIM/ICQ protocol. However, the documentation on the Internet combined with network traffic analysis should be sufficient for third parties to develop a Yahoo! compatible client or server.
Data Packets

A YMSG packet starts with the letters YMSG. If the client sends the packet to the server, the byte that follows will be the version of the protocol. If the server sends it, the following byte will be zero.

For YMSG packets in version nine of the protocol, the header will appear as follows:

- DWORD Message start
- BYTE Protocol Version
- DWORD Unknown
- WORD Length
- BYTE Type
- DWORD Unknown
- DWORD Identifier

Message Start
These bytes are always the letters YMSG, signifying the start of the packet.

Protocol Version
If sent by the client to the server, this value is the version number; otherwise, it is zero.

Length
This byte describes the length of the data that follows the header.

Type
This byte describes the type of packet.

Identifier
This DWORD value identifies the user. This is a pseudorandom number. The client will use this same pseudo-random number during a whole session. Only when the user logs off and logs on again will this number change.

The data is located directly after the 14-byte header. Not all packets contain data. Below is an example of a YMSG packet that does not contain data. This is the first packet sent by the client to the server.

59 4D 53 47 09 00 00 00 00 00 00 4C 00 00 00 00 YMSG…. …L…..
69 2C A8 72 i,.r

Servers and Ports

By default, Yahoo! Messenger connects to cs.yahoo.com on port 5050. If direct access is being blocked, the client will automatically try several other ports. As an HTTP header will be added to the packets, the instant messaging traffic will pass through firewalls even with protocol analysis.
Password Encryption

Yahoo! has used different methods to encrypt the password. Earlier versions used the MD5 crypt function to hash the password before sending it. However, Yahoo! decided to change the MD5 crypt to a more secure method in later versions. Version nine of the YMSG protocol uses a challenge-response method similar to AIM/ICQ.

The Yahoo! server sends the client a 24-character string. The client sends two 24-character strings back to the server. The two strings contain an MD5 crypt hash of the password, as well as the encrypted user name. This is all the information the server requires to verify the user.

Login Process

The Yahoo! client connects to cs.yahoo.com. The server sends a challenge string for encrypting the user name and password. The client encrypts the user name and the password and sends back two 24-byte strings to the server.

Once the server verifies the user, a random X-byte cookie is sent back to the client. The client can now use this cookie for various functions, such as checking when new email arrives (if a yahoo.com email address is being used). Once the cookie is received, the client changes the status to online and is ready for messaging.

MSN MESSENGER (ALSO KNOWN AS WINDOWS MESSENGER)

Protocol
The MSN protocol is generally referred to as MSNP. MSNP is an ASCII-based protocol rather than a binary-based protocol. Thus, everything is sent in human readable text. The latest version is MSNP7.

Information regarding MSNP can be found on the MSN Messenger Web site, allowing third-party interoperability.

Data Packets
The data packets start with various commands in ASCII text. The commands start with three characters, and are followed by the actual information regarding the command that is being sent. Examples of commands are XFR (transfer), USR (user), and CHG (change).

One TCP/IP packet can have more than one command. The commands are separated using carriage-return/linefeed (CRLF). The MSNP package also is terminated using CRLF.

A short example of a communication via MSN Messenger can be found below.

When a user wants to chat with another user, the client sends the following packet to the server:

```
58 46 52 20 39 20 53 42 XFR 9 SB
```

This is a request by the client for a switchboard server. All instant messaging communication occurs on a switchboard server.

The server will respond with a packet similar to the following:

```
58 46 52 20 39 20 53 42 20 36 34 2e 34 2e 31 32 XFR 9 SB 64.4.12 61863 CKI 60
2e 31 35 38 3a 31 38 36 33 20 49 20 36 30 .158:186 3 CKI 60
36 39 37 38 2e 31 30 33 34 36 31 35 30 36 34 2e 6978.103 4615064.
33 31 31 32 39 0d 0a 48 4c 20 30 30 36 34 129 61296534615064.31129
34 31 34 36 31 34 33 35 30 31 32 39 31 32 34 30 41461435 01291240
36 Od 0a 3.
```

Since CRLF (0x0D 0x0A) is used as separators between commands, the packet above can be separated into the following commands:

```
XFR 9 SB 64.4.12.158:1863 CKI 606978.1034615064.31129
```

This is the IP address and port of the switchboard server that the client should use for the instant messaging session. It also contains a security hash that the client must use when connecting to the switchboard server. The security hash starts with the letters CKI.

```
CHL 066541461435012912403
```

This is a challenge key used by the client for authentication. This was introduced in version seven of the MSNP protocol.
Server and Ports

By default, the client will attempt to connect to the server on port 1863. If the client is unable to contact the server directly on this port, it will attempt to use a proxy server. In this case, an HTTP header will automatically be added to the packets. This causes the packets to pass through security measures such as protocol analysis.

Password Encryption

MSN Messenger uses a challenge-response method for sending the password. During the login process, the client requests a security packet, which contains information regarding the method that should be used for hashing the password. In most cases, the client hashes the password together with a server-supplied challenge string using the MD5 algorithm.

The benefit of using a hash together with a challenge key is that the hash sent by the client will not be the same twice. Furthermore, it is extremely difficult to recover the password from a hash sent from the client to the server.

Login Process

Each MSN Messenger session starts by the client and server agreeing on which version of the protocol to use. Once the version of the protocol has been established, the actual login sequence begins.

The client will authenticate with the server by sending the user name and a hash of the password. If the client authenticated successfully with the server, it is ready for instant messaging.

Under version seven of the MSNP protocol, after a successful authentication, the server will send information regarding the user. This is mainly information that can be modified by the user, such as birthday, country, and language. However, it also contains a cookie that can be used for services other than instant messaging.

Threats to Instant Messaging

Threats to instant messengers are not limited to worms, but also include Trojan horses that export data and create back doors into the system. Furthermore, one of the greatest threats of utilizing any instant messenger is simply privacy.

WORMS

Email spreading worms are part of daily life for any computer security professional. Some of the worms have great success in spreading their infection due to social engineering or due to the usage of security exploits. However, these threats can be dealt with swiftly due to antivirus products that monitor email traffic, as well as the normal user being more aware of them. The number of instant messaging worms is rising steadily, but there are still no antivirus applications that directly monitor instant messaging traffic and only a few that directly plug in to instant messaging clients, being notified when a file is received. This is partly due to the difficulty in monitoring instant messaging traffic, as well as the constant modifications to the clients and the protocols that they use.
Unfortunately, this makes instant messengers an open door to the computer, as the traffic will pass most server-based security measures unscanned for potential worms. Only the antivirus product running on the computer itself can catch the worms.

Below is a list of some of the worms that utilize various instant messengers to spread themselves.

- W95.SoFunny.Worm@m
- W32.Aplore@mm
- W32.Goner.A@mm
- W32.Choke
- JS.Menger.Worm
- W32.FunnyFiles.Worm
- W32.Annoying.Worm
- W32.Mylife
- W32.Maldal (some versions)
- W32.Seesix.Worm
- W32.Led@mm
- VBS.Msnb.Worm

More information regarding these worms can be found at: http://securityresponse.symantec.com.

**BACKDOOR TROJAN HORSES**

One can share every file on a person's computer using an instant messenger. All the popular instant messengers have file sharing capabilities, or the ability to add such functionality by applying patches or plug-ins. The benefit for a hacker using an instant messenger to access files on a remote computer instead of installing a backdoor Trojan horse is that even if the computer is using a dynamic IP address, the screen name will probably never change. Furthermore, the hacker will receive a notification each time the victim computer is online. This will make it much easier for the hacker to keep track of and access infected computers. In addition, the hacker does not need to open a new suspicious port for communication, but does so via already open instant messaging ports.

There are a handful of Trojan horse programs that target instant messaging. Some modify configuration settings so file sharing is enabled for the entire hard drive. These types of Trojan horses pose a large threat, as they allow anyone full file access to the computer.

There are also classic backdoor Trojan horses that utilize instant messengers to send messages to the author of the Trojan horse, giving the hacker information about the infected computer. This information includes things such as the IP address of the infected computer and the number of the port that has been opened.

Backdoor Trojan horses that allow file-access to the computer by utilizing instant messenger clients may be harder to discover than classic backdoor Trojan horses. Classic backdoor Trojan horses open a listening or outgoing port on the computer, forming a connection with a remote machine. These classic backdoor Trojan horses can effectively be blocked by a desktop firewall.
However, if the backdoor Trojan horse operates via the instant messaging client, it does not open a new port and thus, is not blocked by traditional desktop firewall products.

Backdoor Trojan horses utilizing instant messengers are already in use today. Recently, a backdoor Trojan horse that sends ICQ pager messages to the author was discovered. It has been named Backdoor.AIMvision, and it allows the hacker to steal information regarding AIM that is stored in the Windows registry. It also allows the hacker to configure the AIM client.

Another backdoor Trojan horse that uses ICQ messages to contact the author is Backdoor.Sparta.C. More information regarding this backdoor Trojan horse can be found under the specific threats to ICQ section.

HIJACKING AND IMPERSONATION

There are many different ways in which hackers can impersonate other users. The most frequently used attack is simply stealing the account information of an unsuspecting user.

Stolen account information for any instant messenger can be very damaging. The people on the victim's buddy list will trust the hacker. Therefore, it will be easier for the hacker to convince the people on the buddy list to run files on their computers or divulge confidential information. Losing a password for an instant messenger account can therefore be dangerous for more people than just the person who lost the password.

To get the account information of a user, the hacker can use a password-stealing Trojan horse. If the password for the instant messaging client is saved on the computer, a hacker could send a Trojan horse to an unsuspecting user. The Trojan horse, when executed, would find the password for the instant messaging account used by the victim and send it back to the hacker. The means for sending back the information to the hacker vary. They include using the instant messenger itself, IRC, and email.

Since none of the four instant messaging protocols encrypt their network traffic, one can highjack connections via man-in-the-middle attacks. By inserting messages into an ongoing chat-session, a hacker could impersonate one of the chatting parties.

Though very difficult, one can also highjack the entire connection by using a man-in-the-middle attack. For example, a disconnect message, which appears to come from the server, can be sent to the victim from the hacker. This will cause the client to disconnect.

The hacker can also use a simple denial of service exploit, or other unrelated exploits, to make the client disconnect.

Since the server keeps the connection open and does not know that the client has disconnected, the hacker can then impersonate the victim user. Furthermore, since all data is unencrypted and unauthenticated, a hacker can use classic man-in-the-middle attacks such as ARP spoofing.
DENIAL OF SERVICE

There are many ways in which a hacker can cause a denial of service on an instant messenger client. Some denial of service attacks make the instant messaging client crash. Other types of attacks will make the client hang, and in some cases consume a large amount of CPU power, causing the entire computer to become unstable.

One common type of attack is flooding a particular user with a large number of messages. The various instant messaging clients do contain a protection against flood-attacks by allowing the victim to ignore certain users. However, there are many tools that will allow the hacker to use many accounts simultaneously, or that will automatically create a large number of accounts to accomplish the flood-attack.

Furthermore, after the flood-attack has started, by the time the attacked user has realized what is happening, the computer may become unresponsive. This makes it difficult to add the attacking user accounts to the ignore list of the instant messenger client.

Exploits that cause a denial of service for the instant messenger client are a common type of exploit. These exploits are potentially the most dangerous types of denial of service attacks, as it may be difficult to protect against them. Furthermore, some of the exploits don’t actually crash the client. Instead, they make the instant messenger client consume a large amount of CPU time. This causes the computer to become unresponsive, rather than just the instant messenger client.

Even though denial of service attacks are more of an annoyance than they are dangerous, they can be used in combination with other attacks, such as the hijacking of a connection.

INFORMATION DISCLOSURE

Tools that attempt to retrieve the system information from instant messenger users are in very common use today. An example of such a tool is an IP address retriever.

IP address retrievers can be used for many purposes. For example, if an IP address retriever was used together with a backdoor Trojan horse, the hacker could receive a message containing the IP address of an infected user each time the victim comes online.

This way, the hacker would know the IP address of the infected user, even if the user were using dynamic IP addresses.

There are many ways in which a hacker can send a data export Trojan horse, such as an IP address retriever, to an unsuspecting user. By using either good social engineering or potentially unrelated exploits, the hacker can make the unsuspecting user execute the file. The data export Trojan horse finds information on the user’s computer and sends it back to the hacker via the instant messaging network.

There are many different types of data stealing Trojan horses available for all of the different instant messaging clients.

For example, a hacker may steal the password for the user’s account. When the user logs out, the hacker has full control over the account. He can perform various tasks, such as changing the password and sending files to people on the buddy list.
In addition, information disclosure could occur without the use of a Trojan horse. Since the data that is being transmitted over the instant messaging network is not encrypted, a hacker could sniff the packets and thereby monitor an entire instant messaging communication. This can be very dangerous. For example, if an employee within a company uses instant messaging to communicate sensitive company data, the hacker could see this communication and thereby get access to the information.

THREATS SPECIFIC TO AIM

Worms

There are many worms that can spread using various instant messaging networks. W32.Aplore@mm is a worm capable of spreading using the AIM network. The worm spreads by sending a message to all of the contacts on the AIM buddy list.

The message will be one of the following:

- btw, download this,
- I wanted to show you this,
- please check out,
- hey go to,
- see if you can get this to work,
- this is cool,
- tell me what you think about,
- try this,
- I almost forgot about,
- I like this,
- what about,
- have you seen,
- interesting,
- lol,
- wow,
- whoa,
- neat,
- cool,
- hmm,
- psst,
- hehe,
- haha,
- silly,
- weird,
There will also be a link in the message that references a Web page. The Web page is hosted on the infected computer, since the worm acts like a Web server running on port 8180.

The Web page will appear as follows:

- **Browser Plugin Required**
  
  You may need to restart your browser for changes to take affect.

- **Security Certificate by Verisign 2002.**
  
  MD5: 9DD756AC-80E057FC-E00703A2-F801F2E3

- **Click HERE and choose *Run* to install.**

Of course, the file that will be downloaded is a copy of the worm.

More information regarding this worm can be found at http://securityresponse.symantec.com/avcenter/venc/data/w32.Aplore@mm.html.

**EXPLOITS**

One type of threat that is being used frequently by hackers is exploits. There are several known exploits for AIM. AOL quickly fixes most of the exploits on the server end by filtering malicious traffic. Therefore, in most cases, users do not need to update their clients to protect themselves from the exploit. However, there are exploits that require a patch on the client end.

The following is a list of some recent exploits:

1. **AIM Link Special Character Remote Heap Overflow Vulnerability**
   - A specially crafted URL string can cause the AIM client to crash.
   - Source: http://online.securityfocus.com/bid/5492/info/

2. **AIM Unauthorized Actions Vulnerability**
   - By adding AIM information in a meta refresh tag on a Web page, the AIM client can be forced into adding groups and buddies on the AIM buddy list.
   - Source: http://online.securityfocus.com/bid/5246

3. **AIM AddBuddy Hyperlink Vulnerability**
   - A large aim:addbuddy link in a Web page can cause the AIM client to crash.
   - Source: http://online.securityfocus.com/bid/4709/info/

At the end of 1999, a tool called AIMThief was being used to steal AIM accounts.

Using an exploit in the AIM protocol, the tool allowed the hacker to input the screen name of a victim. The tool would then change the password for this screen name.

Even though this tool no longer works, it demonstrated the vulnerability of instant messaging systems. Furthermore, such a vulnerability required action by the instant messaging vendor and no workaround or patch existed for the end user.
THREATS SPECIFIC TO YAHOO! MESSENGER

Worms
There are currently no known worms that utilize Yahoo! Messenger.

Exploits
1. Yahoo! Messenger Call Center Buffer Overflow Vulnerability
   - It is possible to insert ymsgr:// links on Web pages. These will be handled by the Yahoo! Messenger application. By making these links very large, one can cause a buffer overflow in the Yahoo! Messenger client.
   - Source: http://online.securityfocus.com/bid/4837

2. Yahoo! Messenger Script Injection Vulnerability
   - If Yahoo! Messenger is integrated with the Web browser, a link can be created that will open up a Web page in the instant messaging client and additionally execute a script of choice.
   - Source: http://online.securityfocus.com/bid/4838

THREATS SPECIFIC TO ICQ

Worms
W32.Goner.A@mm is a mass-mailing worm that has the capability to spread using the ICQ instant messaging network. It is a worm written in Visual Basic, and it has been compressed using UPX.

If ICQ is installed on the computer, the worm will do the following:

1. Check the version of an ICQ DLL file and verify that it contains the APIs that the worm wants to use. If the correct version is found, the worm proceeds.
2. Retrieve a list of all contacts that are currently online.
3. Retrieve information about each user individually. This information is required to be able to send files.
4. Send itself to all users on the list.

More information regarding W32.Goner.A@mm can be found at http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html.

BACKDOOR TROJAN HORSES

ICQ allows users to send messages using a Web browser. Authors of backdoor Trojan horses have begun to exploit this functionality. For example, a backdoor Trojan horse named Backdoor.Sparta.C is a traditional backdoor Trojan horse that opens a port on the computer allowing incoming connections. However, after infecting a user, Backdoor.Sparta.C will send a message to the author using ICQ on the Web. The message that it sends includes information such as IP address, which port is opened, and some information regarding the infected computer.

More information regarding this backdoor Trojan horse can be found at http://www.sarc.com/avcenter/venc/data/backdoor.sparta.c.html.
EXPLOITS

1. ICQ 2001/2002 Malformed Message Denial Of Service Vulnerability
   - ICQ allows insertion of graphical smiles in messages. If a large number of smiles are inserted into one message, the receiving ICQ client will hang for 10–20 seconds, consuming all CPU time. It may also crash instead of hanging.
   - Source: http://online.securityfocus.com/bid/5295

2. Mirabilis ICQ Soundscheme Predictable File Location Vulnerability
   - The default action for an ICQ soundscheme (scm) file is to open it and place the wave files included with the scm file in a known location on the hard disk. The file will be downloaded and installed at the following location: C:\ProgramFiles\ICQ\Sounds\[name]. By knowing the location at which the file will be stored, file execution vulnerabilities can be used. There are such reported exploits for Internet Explorer.
   - Source: http://online.securityfocus.com/bid/5247

AUTHORIZATION BYPASSING TOOLS

In ICQ, one can set whether authorization is required before being added to another user’s contact list. However, there are many tools available that bypass this authorization. This allows unauthorized users to determine another user’s online/offline status.

These tools are able to bypass authorization because ICQ saves the contact list on the local computer, whereas all the other instant messengers save the contact list on the server. The latest version of ICQ also uses the server to store the contact list. However, because of backwards compatibility, a contact list still stored on the local computer can be submitted to the server.

THREATS SPECIFIC TO MSN MESSENGER

Worms

MSN Messenger is the instant messaging network that has the largest number of worms. This is probably due to the large amount of documentation available for the MSN Messenger service, as well as the simplicity with which an application can be created to interact with the service.

One widespread worm that utilized the MSN Messenger network is W32.Choke.Worm.

The worm hooks MSN Messenger so when a buddy initiates a text conversation for the first time with an infected system, the remote system sends the following text message:

   President bush shooter is game that allows you to shoot Bush balzz hahaha

Along with the message is an invitation to download a file named ShootPresidentBUSH.exe. If the buddy declines, the worm repeatedly sends the invitation.

The worm remembers the name of each buddy who has already accepted a copy of the worm and responds with a smiley face to every message sent by that person.

More information regarding this worm can be found at http://securityresponse.symantec.com/avcenter/venc/data/w32.choke.worm.html.
EXPLOITS

1. Microsoft MSN Messenger Malformed Invite Request Denial of Service
   • A corrupted header in an MSN Messenger invite request can cause the MSN Messenger client to crash.
   • Source: http://online.securityfocus.com/bid/4827/info/

2. Microsoft MSN Messenger Message Spoofing Vulnerability
   • Source: http://online.securityfocus.com/bid/4316/info/

3. Microsoft MSN ActiveX Object Information Disclosure Vulnerability
   • Due to a bug in the document.open function, one can read the contact list of a user, and impersonate users. The example code that was submitted with the exploit has been used in a worm. The worm has been named JS.Menger.Worm. More information regarding this worm can be found at http://securityresponse.symantec.com.
   • Source: http://online.securityfocus.com/bid/4028/info/

Blocking Instant Messengers

Preventing the use of instant messaging is difficult. Simple port blocking firewalls will not be effective because clients can use common destination ports such as HTTP port 80 and FTP port 21. Most of the clients will even auto-configure themselves to use other ports than the default one if they are unable to communicate over the default port.

Firewalls with protocol analysis may prevent instant messaging clients from communicating via common destination ports, such as port 80, because instant messaging traffic is different from HTTP traffic. However, the latest versions of all the various clients embed the traffic data within an HTTP request, bypassing protocol analysis.

The client and responses essentially prepend an HTTP header to each packet sent, thereby circumventing any protocol analysis firewall. With some clients, such as ICQ and AIM, HTTP headers are added only when an HTTP proxy must be used. However, AOL provides access to such a proxy for free, namely www.proxy.aol.com, and the clients auto-configure themselves to use this proxy if direct access is being blocked on all ports.

Even though, in the case of AIM and ICQ, access to the proxy can be prevented by blocking the address, there are many other proxy servers freely available on the Internet. A simple search on the Internet will return hundreds of freely available proxy servers. Keeping up with blocking each one is difficult and an administrative nightmare.

Corporate policies are the best way to prevent employees within companies from using instant messaging.
The Future of Instant Messaging

Instant messaging is a communication method that has proven to be a very good complement to the ways in which we communicate, both privately and professionally. Over time, instant messaging clients have become easier to use, and they have begun to incorporate other functionality such as voice communication and file sharing.

The number of instant messaging users is currently in the millions, and more and more people are subscribing to the services provided by the four major networks.

The problems with instant messaging are many, but education and better response from the companies that provide the services can help reduce them. Many of the companies fix exploits on the server end, thereby avoiding the problem of having users apply patches to the clients.

It is surprising that more worms and other types of malware are not utilizing instant messaging. As time progresses, we will very likely see an increase in this area. With time, we may also see more interoperability among the various networks. AOL has already abandoned the ICQ protocol in favor of its own OSCAR protocol. We may see interoperability between AIM and ICQ soon. This interoperability may allow worms to travel among all four networks rather than being confined to a single network.

Privacy issues and the ability to log instant messaging traffic are important features for companies. There are already clients for some of the instant messaging networks that offer encrypted communication. However, only when these features are incorporated into the official clients and the networks that they use can companies begin to rely more heavily on instant messaging communication.

Summary

Because hackers currently are targeting individual users, hackers aren’t a big threat for any instant messaging network as a whole. On the other hand, worms target all users for a particular network, and therefore they appear to pose the biggest threat for the future.

We have seen that worms that use security exploits can become widespread in a very short amount of time. Code Red and Nimda are examples of worms that used security exploits to spread themselves quickly.

In the near future, instant messaging is not likely to be as big a carrier of worms as email is today. Email is currently used by more people than instant messaging, and thus worms spread to a larger audience using email. If a worm sends itself to all contacts in your address book, it potentially sends itself to every employee in the company for which you work. However, if the same worm spreads itself to every contact on your instant messenger list, it would probably not reach more than a handful of people.

Furthermore, the major instant messaging networks still use proprietary protocols. Since they are all different, a worm that spreads using MSN Messenger will not affect users of the Yahoo! Messenger service. If clients become interoperable, or users primarily utilize one network, instant messaging worms may become more widespread.
However, this does not mean one can disregard the threat that instant messaging poses. Already, more than 20 worms can spread via instant messaging. There are also many exploits available for the various clients.

In the future, it appears that exploits will be the predominant way hackers attack a system. If different instant messengers become interoperable, the security track record of a vendor may decide which instant messenger a company chooses to use.

Email traffic within companies is generally monitored by antivirus software. Therefore, once detection is available for a particular worm, infected emails will be stopped at the server. In the case of instant messaging, antivirus software currently does not monitor traffic at the gateway level. If a worm started to spread using instant messaging, it could not be stopped before it reached the user’s computer.

The number of worms for instant messaging is increasing each month, and looking at the success of some of these worms, clearly instant messaging is an up and coming platform for malicious threats.

We should be careful when using instant messengers and the best way to make sure we can use them safely is by educating users. Hopefully we will never see an outbreak of a worm that can spread using instant messengers only.
SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM