



Raytheon Oakley Systems

USE CASE — MONITORING AND INVESTIGATING INSTANT MESSAGING INSIDER THREATS

A Popular way to Communicate

Many people think that, because of the almost immediate two-way nature of instant messaging communication, it will lead to higher productivity. As a result, IM is increasing in popularity in both professional and personal circles. However, as with most things Internet-based, the increasing use has led to an associated increase in the number of security risks.

Instant Messaging Security Threats

Instant messaging networks provide the ability to transfer text messages and to share or transfer files. Consequently, instant messengers can be a source of information leaks or transfer worms and other malware. Instant messengers 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.

Examples of how this can adversely effect an enterprise include:

- ▶ **Information Leaks** – With no ill intent, an instant messaging user can become a source of information leaks because most instant messaging clients have Peer to Peer networking technologies that can share all files on the system with full access to everyone. Whether they accidentally enable this, or some kind of Trojan infiltrates their system, it can enable other people and in this way gain backdoor access to the computer and its data. In addition, since Instant Messages are usually unencrypted, someone with technical know-how can sniff instant

messaging sessions and read messages that may contain confidential information.

- ▶ **Deliberate Theft of Data** - A user can deliberately send confidential information or intellectual property through instant messaging, knowing that corporate email systems will keep archives and logs that document messages, in an attempt to avoid any documentation of the act
- ▶ **Electronic fraud** - Hackers can impersonate other users in many different ways. The most frequently used attack is simply stealing the account information of an unsuspecting user. Stolen account information for any instant messenger can obviously be very damaging. Because the hacker can use this information to disguise himself as a trusted user, the people on the victim's buddy list will trust the hacker and may therefore divulge confidential information or to gain access to other systems such as a database by finding out enough information about it to hack in.
- ▶ **Denial of Service** - Instant messaging may make an enterprise network or an individual user's computer vulnerable to denial of service (DoS) attacks. Instant messaging can rapidly spread malware and viruses that may have different end results: some DoS attacks overload the network with noise to bring it to a crawl, while others attack individual computers to make them crash hang, and in some cases consume a large amount of CPU power, causing the entire computer to become unstable.

Monitoring Instant Messaging

Raytheon Oakley Systems can help to eliminate both accidental and deliberate disclosure of confidential information and intellectual property by monitoring instant messaging for key data elements such as

USE CASE — IM

MONITORING AND INVESTIGATING INSTANT MESSAGING INSIDER THREATS

Social Security numbers (SSN) or Personal Identifiable Information (PII) such as account numbers, or even types of files such as CAD files that might contain proprietary product specifications or details.

Oakley provides both network-based and agent-based solutions that will each help solve problems associated with instant messaging. CoreView, a network monitoring appliance, can detect when Instant Messages contain expressions such as SSNs and PII and alerts you of the occurrence as to the sender and the recipient of the message.

Should you wish to more closely manage high risk users or want to more closely investigate IM activity for an individual, Oakley's SureView solution will help you take a much closer look and document the activity. The IM collector in SureView's client agent allows you to see complete details of IM threads and make full contextual determinations of both accidental or deliberate disclosure because it allows you to obtain data from the most popular instant messaging clients, such as Yahoo, MSN, AIM, Lotus Notes SameTime, and ICQ. The SureView agent can take an action you desire when such expressions such as SSNs are detected such as collect keystrokes or even on-screen video as users enter text to be sent and any replies received.

The video capture works by watching for the appearance of the unique windows of the different IM applications on the screen. When it detects an IM window, it hooks the windows (rather than the application) and collects the input and output for the different applications.

Stopping IM in its Tracks

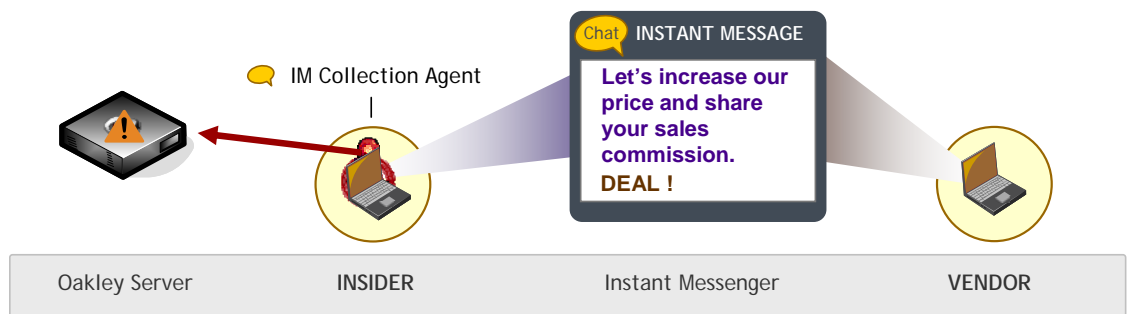
Some organizations believe the most effective way of preventing instant messaging from jeopardizing the security of a network and the machines upon it is to deny it access to the network in the first place. Preventing the use of instant messaging is difficult. Simple port blocking firewalls will not 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.

Raytheon Oakley Systems SureView is able to stop instant messaging by killing the instant messaging application process. When Oakley security agents are deployed on client systems the agents can monitor the processes running on the clients and kill the IM client process when it is detected.

Conclusion

Every organization must determine its own rules and policies for whether instant messaging is allowed in the organization and under what conditions. Oakley Network solutions will monitor for user compliance with these policies and enforce the rules that the organization wants followed.

Through policy-driven monitoring of instant messaging Oakley will help the organization manage risks associated with this often useful, but potentially risky, form of communication.



Obtain data from the most popular instant messaging clients, such as Yahoo, MSN, AIM, Lotus Notes SameTime, and ICQ

Raytheon Oakley Systems
 2755 Cottonwood Pkwy., Ste. 600
 Salt Lake City, UT 84121

T 1.800.662.9120
 E info@oakleynetworks.com

www.raytheonOakleySystems.com

Raytheon
Oakley Systems