

IMlogic

IMlogic Threat Center

2005 Real-Time Communication Security:
The Year in Review

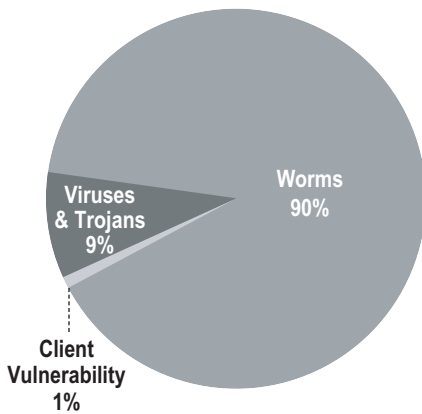
IM makes it possible
IMlogic makes it work

Introduction

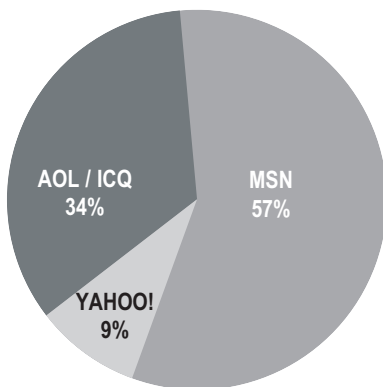
Instant Messaging continues to be the fastest growing communications medium of all time with an estimated 300 million consumer and enterprise IM users in 2005. Global services such as AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger each report over 1 billion messages sent per day, and IM traffic is expected to exceed email traffic by the end of 2006. As one of the most successful and widely-deployed applications on the Internet, IM has increasingly become the target for attackers to propagate IM-borne viruses, worms, spam over IM (SPIM), malware and phishing attacks. Though widespread in adoption, IM is generally unprotected and unmonitored in consumer and enterprise environments, leaving it vulnerable to attacks and exploits. These attacks have grown exponentially over the past 3 years, increasing the need for real-time threat protections for IM and other real-time communications applications. The IMlogic Threat Center, the industry's first global consortium to provide threat detection and protection for instant messaging (IM) and real-time communication applications, publishes this annual report of Real-Time Communication Security Threats to provide a round-up of the threats from the previous calendar year.

The findings included in this report are based on research and analysis of the threat information reported and tracked by the IMlogic Threat Center and its partner community. Incidents reported to the IMlogic Threat Center include open forum submissions from the general public, IMlogic enterprise customer events, IM threat diagnostics and signature definitions from the IMlogic Real-Time Threat Protection System (RTTPS), IMlogic Threat Center Global HoneyPot Network events, and data contributed from consortium members, representing industry leaders in Internet Security and Instant Messaging. The 2005 IMlogic Threat Center Real-Time Communications Security Threat Report covers data captured between January 1, 2005 and December 31, 2005.

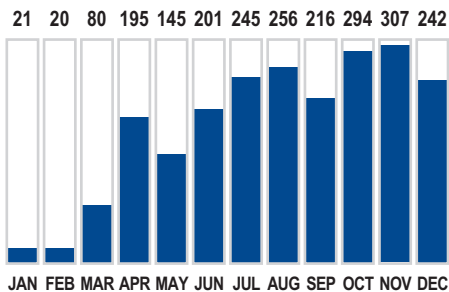
Threat Types



2005 Reported Threats by IM Network



IM Threats Reported 2005



2005 Real-Time Security Threats in Review

In 2005, real-time security threats associated with instant messaging, peer-to-peer and other real-time communication technologies increased 1693% over 2004, with a total of over 2400 unique threats. As both legitimate and unapproved use of instant messaging clients, peer-to-peer applications and other real-time communication appliances increases, new worms and viruses are increasingly using these mechanisms to propagate and cause widespread damage. IM worms are the most prevalent form of IM malware, representing 90% of all unique attacks in 2005. These attacks frequently utilized social engineering techniques to lure end users into clicking on suspicious links embedded inside IM messages, enabling the activation of malicious code that compromised the security of host operating systems or applications. In 2005, IM virus infections through file transfer represented 9% of unique real-time security threats. The use of peer-to-peer file transfer capabilities is likely to become more widely used as a threat vector as IM file transfers in the enterprise bypass traditional gateway and email antivirus security systems. AOL, MSN and Yahoo! client vulnerabilities represent the remaining 1% of unique threats. For the year, 2005 reported data includes:

- 1693% increase in reported incidents of new real-time security threats
- 2403 unique IM and P2P threats, including IM-specific attacks and blended threats which target IM and P2P applications
- 90% of IM-related security attacks included worm propagation; 9% are known to have delivered viruses; and 1% of reported incidents utilized known client vulnerabilities or exploits
- 57% of reported incidents over IM networks targeted the MSN Messenger Client, Windows Messenger Client and MSN Network
- 34% of reported incidents over IM networks targeted the AOL Instant Messenger Client, AOL Instant Messenger Network, ICQ Client and ICQ Network
- 9% of reported incidents over IM networks targeted the Yahoo! Messenger Client and Yahoo! Messenger Network

In addition to the overall increase in the volume of real-time security threats, 2005 saw a dramatic increase in the overall sophistication of these threats. With this increase the overall depth and breadth of the damage caused by these threats dramatically rose. As part of the increased risks associated with these threats, the following are highlights from 2005:

- The first talking, “intelligent” worm was identified (IM.Myspace04.AIM). This worm not only broadcasted malicious messages to other users of IM but also interacted with potential victims without the infected user’s awareness of the messages as an attempt to dupe potential victims into activating the worm on their own local machine.
- A dramatic increase in the number of mutating attacks, including significant mutations on all the major consumer IM networks. With 140 total mutations and detection on all the major IM networks, the Kelvir worm was the leader in IM threat mutations, followed by Bropia with 29 mutations and Opanki with 26 mutations. In fact, one Kelvir mutation forced a temporary shutdown of the Reuters Messaging network.
- Rootkit technologies became one of the mechanisms attackers leveraged to hide their malicious code and malware on infected machines. In one instance that occurred late in the 2005 Holiday season, attackers used rootkit technology in a worm disguised as the “Santa” worm, also known as the Christmas gift worm, to attack unsuspecting IM users. This worm attempted to dupe users into visiting a Web site that appeared to be a harmless Santa Claus site but in actuality distributed a malicious payload to the end-user.
- During the year, the overall level of sophistication demonstrated by IM attacks increased, including worms that took advantage of multi-stacked clients (for example, Windows Messenger) and included support for multiple languages to enable threats to more easily traverse geographic and regional boundaries. In one instance, the Kelvir-ASVID worm, propagated over Microsoft Office Communicator, MSN Messenger and Windows Messenger, causing widespread infection of Windows machines and significant disruption and damage inside enterprise IT domains.

Top Threat Mutations in 2005

One of the most alarming trends from 2005 was the increase in the number and prevalence of IM threat mutations. As a result of this increase, the IMlogic Threat Center started tracking threat mutations as a key indicator of IM security risk. The following list of IM specific threat mutations were the most widely reported in 2005:

Group	Latest Variant	Latest Posting	First Reported	Variants	Distribution Method
Kelvir	W32/Kelvir-BJ	12/21/2005	2/25/2005	140	All IM
Bropia	Bropia-K	12/22/2005	1/19/2005	29	MSN
Opanki	W32/Opanki-W	12/8/2005	5/6/2005	26	AIM, IRC
Chode	W32/Chode-Q	12/27/2005	3/18/2005	16	AIM, IRC, MSN
Rbot	W32/Rbot-BDV	1/6/2006	1/1/2004	16	AIM, IRC

Overall, the 2005 threat data reinforces IMlogic Threat Center reports, as well as observations and recommendations from other third party sources and security experts, that many existing enterprise IT security protections are insufficient for protecting organizations against the threats posed by real-time communications. In many instances of IM worm outbreaks in 2005, these worms continue to demonstrate that traditional anti-virus software is not sufficient to protect end-users and organizations against the rapid mutation and spread of the latest real-time security threats. Traditional anti-virus products rely on known threat signatures to protect organizations, often relying on reactive mechanisms to update threat signatures after an outbreak has already been identified. In 2005, the rapid proliferation of real-time security threats makes it increasingly more difficult for traditional reactive security approaches to keep pace. The inherent real-time nature of IM, combined with the trend of increasingly destructive IM attacks, highlights the increasing levels of risk organizations are exposed to by unprotected usage of real-time communication applications.

Major IM Security Trends for 2005:

IM Threats Continued to Accelerate as Overall IM Adoption Grew

This past year demonstrated tremendous growth in the overall volume of instant messaging threats, with 2006 most likely continuing this trend. IM threats grew by 1693% in 2005, with more than 2400 known real-time security threats by year's end. IM is the fastest growing communications medium in history, and the threat landscape will continue to mirror that growth. The growth of consumer IM and real-time communication applications will continue, spurred by new entrants and innovations from players such as Google, Microsoft and Skype. Additionally, enterprise-class IM and real-time communication platforms, including Microsoft's Live Communications Server and IBM's Lotus Instant Message platform, will also expand their footprint inside corporate networks.

Attacks Migrated from Simple Vandalism to More Sophisticated Cyber Crime

In the first half of 2005, many IT departments focused on minimizing the cost of repairing infected user machines as this was often the extent of the damage done by attacks. However, as 2005 progressed the damage done by IM attacks increased dramatically in breadth and depth. As IM proved itself to be an efficient and effective delivery vector for malware, the payloads of IM worms and viruses increased in sophistication and were more often designed by cyber-criminals and professionals, not simply mischievous hackers.

Once an IM-related virus or worm infects a user, everything that an end user stores on the computer or does with the computer can be compromised. Confidential information, social-security numbers, bank codes, passwords and other sensitive information that are stored or accessed by the end-user are all vulnerable to theft. With this kind of incentive in place, professionals are recognizing the value of exploiting real-time communications. Although damage to endpoint computers is still the number one financial risk associated with cyber-attacks, the overall financial impact of the theft of proprietary data is on the rise and has eclipsed denial-of-service attacks as the second most costly threat category, according to the FBI and the Computer Security Institute.

About IMlogic, Inc.

IMlogic, Inc. is the market leader in enterprise software for managing and securing instant messaging; the world's fastest growing communications medium of all time. The largest Fortune 1000 companies across the financial services, energy, healthcare, government, media, telecommunications, technology, and manufacturing industries depend on IMlogic to manage, control and secure corporate IM usage, while satisfying compliance requirements associated with real-time electronic communications. For more information on IMlogic call 877-IMlogic or visit www.imlogic.com.

About the IMlogic Threat Center

The IMlogic Threat Center is the first operation to provide detection, analysis, alert, and protection from harmful IM and P2P threats including IM-borne viruses, worms, SPIM, and malicious code. Launched with the support of Internet security leaders Symantec, Sybari, and McAfee, and global instant messaging leaders America Online, Microsoft and Yahoo!, the IMlogic Threat Center is the comprehensive knowledge base for known IM and P2P vulnerabilities and provides rapid response and guidance for protection against newly detected threats.

IM-based Malware Increased in Overall Level of Sophistication and Relevance

IM attackers continued to evolve their malicious payloads thereby improving their ability to propagate, infect and distribute malware, resulting in higher rates of enterprise IT damage and business disruption. Similar to how early email attacks were tests for the effectiveness of infection and propagation, IM threat authors initially tested IM's effectiveness as a delivery mechanism. Like in email, once the vector was proven successful, the virus writers moved quickly to distribute more dangerous and destructive malware.

Recent attacks like the interactive IM worm, which imitated the host by engaging other IM users in dialogue, demonstrated the creativity of today's virus and worm writers to utilize the social engineering aspects of IM to increase infection rates. Many threats are even multi-lingual, speaking to recipients in their native tongue. The social engineering aspect of IM threats, combined with the sense of trust between IM buddy list contacts, have been recognized by attackers as new opportunities for increasing attack sophistication.

In 2005, threats also became more agile than their early predecessors. Threats crossed from one network to another and also from public IM networks to internal, enterprise IM environments. This mobility is especially relevant given the trend toward IM interoperability and federation. As these disparate IM networks and domains are integrated, whether directly through interoperability or indirectly through federation points, the rate of IM and real-time security attacks will continue to increase, matching the increase in number of users on or accessibly by the network of users. Rootkit software, threat mutations, sophisticated communication techniques and agility in disabling reactive security protections and antivirus systems are being included in the new toolset used by attackers.