

[Windows Live Messenger Friendly Infections](#)

Also ICQ, Yahoo IM and AIM

Browsers and operating systems are still the preferred avenue for attacks, vulnerability exploits and spreading malicious code. But at the same time, the consistent effort poured by developers to bulletproof the main attack vectors from Windows Vista to Linux, and from Internet Explorer 7 to Firefox, means that malware needs to find alternative open doors in order to compromise and infect computers. Attacks are shifting away from traditional targets such as Windows and IE and onto third-party applications including instant messaging clients. In this context, security company Sunbelt Software pointed to the discovery of a new piece of malware spreading through the most popular IM clients on the market including Windows Live Messenger, ICQ, Yahoo IM and AIM.

"A relatively new naughty little worm courtesy of Seedcorn Advertising (IM-Worm.TopInstalls.A) does nothing noticeable upon infection, but if you've got ICQ, Yahoo IM, AIM or MSN Messenger, it automatically sends all of your buddies a link to an installer for a full infest of bundled adware/malware," revealed [Alex Eckelberry](#), President Sunbelt Software.

The worm, once it has infected a system, is designed to spread itself via messages sent to all the friends in the contact list. As you can see from the adjacent image, the message containing a link to the malicious code is put together as not to rise any suspicions that it might be anything than what it is pretending.

"Hey, install this ICQ fix to make sure we'll have stable conversations, I already did. [Link] Make sure you installed it before write me – otherwise, without this fix my IM crashes and I can lost contact list," reads the message sent out by the IM-Worm.TopInstalls.A worm to a potentially new victim. Unlike attacks that rely on security bugs, IM-Worm.TopInstalls.A does not exploit a vulnerability in the instant messaging clients.

Instead, it preys on the trust of IM users in a new nuance of an old trick from the social engineering bug. Such a recommendation from a friend is hard to ignore, and even harder not to carry out, becoming infected in the process. Just be sure to pay extra attention to such messages, and always look for dissonant elements, like flagrant spelling and grammatical errors that generally give out a fake message.