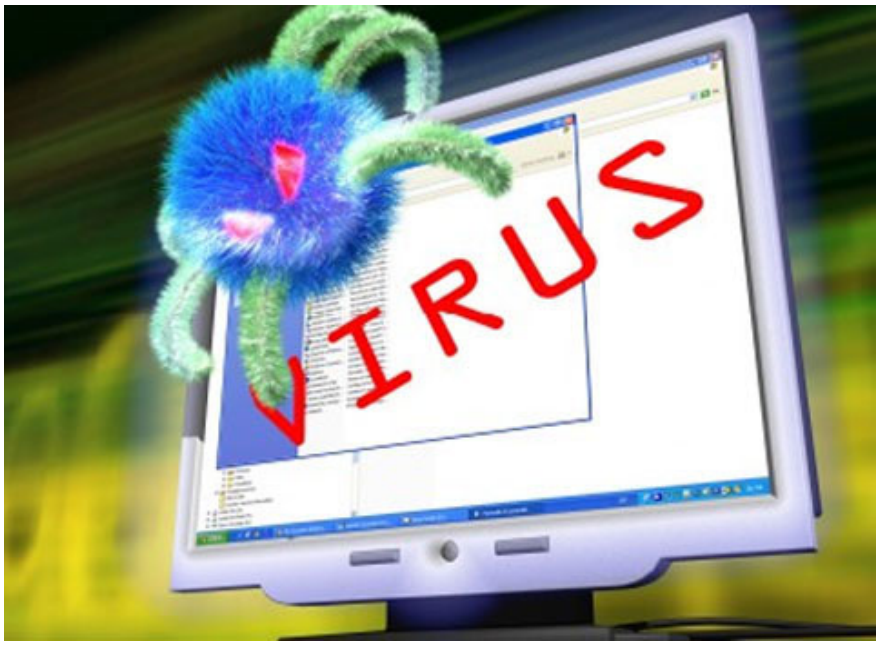
# Dangerous virus attacks the chat program

Kaspersky Lab has discovered a worm called IM-Worm.Win32.Zeroll with 4 variants that can spread in all chat programs such as Yahoo Messenger, Skype ...

**Kaspersky Lab has discovered a worm called IM-Worm.Win32.Zeroll with 4 variants that can spread in all IM programs such as Yahoo Messenger, Skype or Windows Live Messenger.**




*Artwork: Internet*

The mechanism of this virus activity is similar to many other types that have appeared and disturbed the online community in Vietnam before. When a computer is infected with this virus, it will automatically replicate itself to all other chat buddies on the victim's list. 'Decoy' sent to other victims is a link that seems to lead to a very attractive image but actually a file containing malicious code. Curious users who click on this link will be infected with the virus. So the virus spreads quickly on the network.

What makes this worm capable of spreading quickly is that it can appear in many different languages ??(13 languages) and spread through popular chat programs: Yahoo! Messenger, Skype, Paltalk Messenger, ICQ, Windows Live Messenger, Google Talk .

**IM-Worm.Win32.Zeroll** worm has the ability to 'backdoor', ie, after infecting the victim's computer, it will automatically contact the hacker remote control center to receive a real command. Show the action. It can automatically download many other malicious programs on computers that the victim is still unaware of. Hackers can turn these infected computers into a massively hacked computer network for them to perform

attacks or spam. Currently Kaspersky Lab products have been updated and can disable **IM-Worm.Win32.Zeroll** worm **.**

**August: a series of Windows vulnerabilities are exploited**

According to Kaspersky Lab's August 2010 report of malicious code, the security holes of Windows operating system are the number one goal of exploiting and deep attacks.

August saw a strong development of malicious code targeting a vulnerability called *CVE-2010-2568.* This vulnerability was first exploited by the **Worm.Win32.Stuxnet** worm, which is well known for the name 'shortcut' virus. Next is **Virus.Win32.Sality.ag** , a Trojan-Dropper program used to install the latest Sality virus variant.

The CVE-2010-2568 vulnerability that occurs in shortcut files with the LNK and PIF extensions allows worms to spread through infected USB devices.

The three programs directly related to the CVE-2010-2568 vulnerability all appear in the rankings of malicious codes that are regularly blocked in personal computers. Two of them were exploits with **Exploit.Win32.CVE-2010-2568.d** (ranked 9th) and **Exploit.Win32.CVE-2010-2568.b** (12th place) were aimed directly at the security hole.

The other program is **Trojan-Dropper.Win32.Sality.r** (17th place) uses vulnerabilities for propagation purposes. It creates vulnerable LNK shortcut files with names that draw attention and spread across local networks. The malicious code will be activated when the user opens the folder containing one of these shortcuts.