

The new worm attacked AIM and caused heavy damage

A security company has just warned of a new computer worm that is spreading strongly through AOL's AIM instant messaging application and causes more damage than imagined.



A security company has just warned of a new computer worm that is spreading strongly through AOL's AIM instant messaging application and causes more damage than imagined.

According to FaceTime Communications, the new worm is still unnamed in order to spread a lot of malicious software, including rootkits. (Rootkits are a tool designed to overcome security barriers to take control of a computer to open the door for an attack.)

Tyler Wells, a senior expert at FaceTime, said that when users click on a link that the new worm impersonates, a series of malicious software will be downloaded to the user's computer. This is also the first time this security firm has discovered a rootkit attached to a group of malicious software distributed through computer worm. This is a worrying new trend.

In recent times, the number of attacks by computer worms or dangerous code types through instant messaging services is growing rapidly. According to a recent report by security firm Imlogic, the number of network security threats detected on P2P or instant messaging networks has increased by 3,295% in the third quarter of 2005 over the same period. last year.

Besides the 'lockx.exe' rootkit attached to the attached malicious software, there is also Sdbot, FaceTime trojan. This trojan is responsible for opening the following public on infected computers. Not only that, the worm also

downloads users with a variety of ad spyware such as 180Solutions, Zango, the Freepod Toolbar, MaxSearch, Media Gateway and SearchMiracle.

And it is these dangerous software that consumes resources on users' computers, making the system slow. Not only that, these dangerous software also have the function of disabling any anti-virus security applications or changing the browser's home page, default search page.

Computer worms spread through IM networks often have a very fast dispersion speed. We forged the ID name in the buddy list in the instant messaging application as a harmless message but it was really dangerous for the software that came with it.

Advice for users should be careful when clicking on a link on messages and regularly updating antivirus software. The best advice for you when you receive an instant message containing a link is that you should reassure the sender or not click indiscriminately.

You finished reading the article "**The new worm attacked AIM and caused heavy damage**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.