

Rootkit malicious program appears in IM

Security experts have warned about a new worm that has not been named in the instant messaging system (IM). It is a mixture of unwanted software, including rootkits, tools to exploit unprotected parts in the

Picture 1 of Rootkit malicious program appears in IM

Security experts have warned about a new worm that has not been named in the instant messaging system (IM). It is a mix of unwanted software, including rootkits, tools to exploit unprotected parts in your computer.

'When you click on a link that contains a worm, a program containing an attack code will quickly infiltrate your system,' said Tyle Wells, the company's technical director, FaceTime (USA). 'This is the first time we have seen that rootkits act as a package of dangerous applications that are sent to the computer via IM. This trend is not pleasant at all.'

In addition to the lockx.exe rootkit file, the worm also releases a version of Sdbot. This Trojan will open a backdoor on the infected computer so that hackers can remotely control the system. It also leaves behind some spyware and adware applications, including 180Solutions, Zango, Freepod Toolbar, MaxSearch, SearchMiracle and Media Gateway.

All "uninvited" software will exploit the entire system resources, slow down the computer, disable security programs and change the search page on the user's browser. New worms are only found in AOL instant messaging system chatrooms.

IM attacks with worms and malicious code are going on with denser density than before. According to US security provider IMlogic, the number of risks in instant messaging and P2P peer-to-peer networks increased by 3.269% in the third quarter of 2005 compared to the same period last year.

You finished reading the article "**Rootkit malicious program appears in IM**" 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.