Add a computer worm taking advantage of the error MS06-040

Yesterday, Symatec warned of a new computer worm targeting the security bug MS06-040 that appeared on the Internet. New computer worm - named 'Randex.gel' - belongs to the line

Yesterday, Symatec warned of a new computer worm targeting the security bug MS06-040 that appeared on the Internet.

The new computer worm - named " *Randex.gel* " - belongs to the ' *network-ware* ' computer worm line. The network-ware worm is a worm that can be remotely controlled via IRC (Internet Rely Chat) channels and automatically scans the internal network for infection. Therefore, the main function of the worm Randex.gel is to open a back door on infected systems to wait for the control command from their 'owner' via IRC channel.

Oliver Friedrichs - Symantec's director of security response group - said this could be a variant of the Randex worm. The only difference with that computer worm line is Randex.gel that can exploit the security bug MS06-040.

Previous variations of the Randex worm line targeted other security vulnerabilities in Windows such as MS04-007, MS05-017, and MS05-039 - these errors have been fixed by Microsoft.

Friedrichs stated that the code that plays the role of exploiting security bugs mainly in the depth of Randex.gel is very different from other variants. In fact, this code is very similar to the code of HD Moore security researcher

released two weeks ago.

Symantec said the Randex worm could spread in a lot of different ways like through MSN Messenger, AOL Instant Messenger, Yahoo Messenger, and ICQ. The Randex.gel worm can also be distributed through Microsoft SQL servers. If the Randex.gel worm finds a SQL server, it will immediately infect all databases located on that server.

Another function of the worm Randex.gel is to steal personal account information of eGold electronic payment service users when users log into egold.com website.

Although there are many such malicious functions, the Randex.gel worm cannot cause much damage because Microsoft has released the above security patch update.

Hoang Dung