# The new worm attacks Yahoo Messenger users

Security firm Bitdefender has announced a new worm called Worm.Sohanat.Z that infects Yahoo Messenger multimedia messages by enticing users to click on links.

**Security firm Bitdefender has announced a new worm called Worm.Sohanat.Z that infects Yahoo Messenger multimedia messages by enticing users to click on links.**

Worm.Sohanat.Z is a 26th variant of their Sohanat worm. When the computer is infected, there will be the following symptoms:

- Internet Explorer home page will be the website with the virus installed and the victim will not be able to change the homepage because the worm has blocked this function. Refer to the key:

" *HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerMainHome page* "

- Task Manager, Regedit and the Run dialog in the Start menu are also locked

- Automatically send links that infect everyone on the victim's Yahoo Messenger address list. They will be very clever to lead the victim to click on the link to duplicate themselves. This process you will not be able to know unless there is a response from the person who has been infected from the link sent by the virus itself.

In addition, the worm detects the Bitdefender.exe file to see if it is present in the Windows directory. If not, it will download a copy and place it in the% WINDIR% folder. Worm.Sohanat.Z also wants to make sure that it will be automatically activated when Windows starts by editing the value key in the registry: " *HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRunTask Manager* "

Yahoo Messenger users need to be more alert with links sent from the contact list.

The following value keys in the registry will be deeply modified:

- 4 keys have been changed to deep link:

" *HKEY_CURRENT_USERSoftwareMicrosoftSearch AssistantDefaultSearchURL* "
" *HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerMainSearch Page* "
" *HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerMainSearch Bar* "
" *HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerSearchUrl* "

- 3 value keys are changed to 1 (lock).

" *HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosoftWindowsNTSystemRestoreDisableConfig* "
" *HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystemDisableTaskMgr* "
" *HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPoliciesSystemDisableRegistryTools* "

- Value changed to 0 to lock the following settings:

" *HKEY_CURRENT_USERSoftwareGoogleGoogleToolbarNotifierShowTrayIcon* "
" *HKEY_CURRENT_USERSoftwareGoogleGoogleToolbarNotifierKeepDS* "
" *HKEY_CURRENT_USERSoftwareGoogleGoogleToolbarNotifierShowTrayIcon* "

- Search support function is also locked at value:

" *HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerMainUse Search Asst* "

" *The trick of this worm is to disguise a security-related component that is trusted. It exploits the mistake of previous users and then takes advantage of technology errors* ," said Mihai Cimpoesu , virus researcher at Bitdefender said.

Bitdefender recommends that users should update the latest database for their anti-virus, which will prevent and kill this worm.

**Thanh Truc**