Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by light on Sun, 24 Sep 2006 01:57:50 GMT
View Forum Message <> Reply to Message

Yes, I believe it's a false positive.

Quote:W32/Surila-B is a network worm which may try to send a link to itself or W32/MyDoom-W to ICQ contacts.

W32/Surila-B places the main component of itself as dx32cxlp.exe to the Windows system folder and the All Users' startup folder, and as systemst.exe to the Windows system folder. The worm also drops other components of itself to iexpl1orer.exe and SVKP.sys in the Windows system folder.

W32/Surila-B creates the following registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
iestart = <path to iexp1orer.exe>

Additionally W32/Surila-B creates a service named SVKP which causes the file SVKP.sys to be executed when the service starts, for example at system startup.
http://www.sophos.com/virusinfo/analyses/w32surilab.html

Renguard uses SVKP.sys for protection against is being decompiled by cheater (IIRC). SVKP.sys is not a danger to your system.