Subject: Re: Rootkits and Renguard
Posted by Olaf van der Spek on Wed, 09 Nov 2005 14:27:19 GMT
View Forum Message <> Reply to Message

Blazer wrote on Wed, 09 November 2005 03:36All rootkits are essentially the same in that they are trojans that open backdoors and also do their best to hide themselves. Probably the best way to detect a trojan is running some sort of firewall software that pops up when an application tries to access the internet. These sorts of firewalls are a real pain when you first set them up, as you get frustrated having to allow normal system access like "svchost" and the random "rundll32". After a week or so of letting the firewall learn what should be allowed to connect though, it's great for catching trojans that a virus scanner would miss.
Any anti-virus/firewall that runs on the same OS as the rootkit can not be trusted.