Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 19:58:19 GMT
View Forum Message <> Reply to Message

Olaf van der Spek wrote on Wed, 09 November 2005 09:27Any anti-virus/firewall that runs on the same OS as the rootkit can not be trusted.

I would rather have local anti-virus and firewalls, than to trust one central firewall/antivirus, which, once compromised, exposes your entire LAN.

There is no foolproof firewall, the best thing one can do is to be aware of your network connections and OS activity. Even if you had a central firewall that blocked outgoing connections from your PC, it still has to let *something* through, or you wouldn't be able to check email, log into IRC, etc. So then all the attacker has to do is trick you into downloading a rootkit/trojan that sends data out through ports you have permitted, and/or use various methods like arp poisoning.

In short, the only completely secure PC is one that is not connected to the internet in any way, has no USB, floppy, or CDROM drives, and locked behind a cage so there is no physical access.