Subject: Re: Rootkits and Renguard
Posted by JPNOD on Wed, 09 Nov 2005 20:21:47 GMT
View Forum Message <> Reply to Message

[quote title=Blazer wrote on Wed, 09 November 2005 14:52]JPNOD wrote on Wed, 09 November 2005 09:22Yep...

And I would like to add, people running Windows Firewalls and thinking they are safe, well guess what your not. It does not check outgoing c0nn, so run a real firewall.
Or let's say you download a program there might be a botnet in it, not being detected by a virusscanner.. WIndows firewall will just let it trough.
Windows Firewall, does block most worms/trojans. but incomming obviously. (think of msblaster at that time).
Running a Hardware firewall (like a router is a plus), but a software firewall is needed.

This is absolutely false. Most windows firewalls explicitly check outgoing connections, and this is the best way to detect trojans and the like. As I explained, ANY program which initiates any network connection (TCP or UDP) causes a popup and tells you which application is doing it and if you should temporarily or permanately allow it.

Uhhh, With Windows Firewalls I actually just meant the Windows Built in Firewall which comes with SP2, and was already in but with less options and which is also built in Windows Server 2003.

For example, run brenbot, and it windows firewall wont notice it going out. Use zonealarm, or sygate and it will see it straight away. I do agree on that a pc connected to the Internet is nowhere near 100% safe, but if you don't have anything important on it or whatsover. It is really not worth bypassing all this??

http://www.techimo.com/photo/data/500/12firewall.jpg