Subject: Re: Rootkits and Renguard
Posted by Blazer on Wed, 09 Nov 2005 19:52:42 GMT
View Forum Message <> Reply to Message

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.

This sort of firewall is how I discovered the "FlyingBuzz Trojan" years ago (it was a trojan that stole your renegade serial number and posted it to FlyingBuzz's website).

As for "real firewalls" being hardware-based, that is also not entirely true. Most routers, including the cisco router I have in my home network just have "ACL's" (Access Lists), that restrict access by IP subnets.

Also, a certain large ISP that I used to work for did extensive testing and found that a software firewall (OpenBSD + IPF), far outperformed all of the tested hardware-based products

That being said, again I want to stress that using a windows firewall more than likely DOES check outgoing connections, at least I have not used one that does not, including Kerio, Norton, ZoneAlarm, BlackIce, etc.