Subject: Re: new problem with renguard
Posted by totalhavok on Sun, 17 Dec 2006 11:23:19 GMT
View Forum Message <> Reply to Message

Blazer wrote on Sat, 09 December 2006 05:56Go to your services menu (start, run, services.msc), and make sure the SVKP service is started.

OK MAJOR problem HERE!!! svkp.sys!!!! This shows up as SPYWARE!
I just did a fresh install, and as soon as I put renguard back on, ALL my spyware scanners light up like a Christmas tree!!!

Long story short, the idiot the owns the machine I play on was stupid enough to install Kazaa, let Yahoo messenger, MSN, AOL aim, and Quicktime, start up automatically on each reboot. While running the default XP firewall (junk), and some stupid AV-Free anti-virus program that couldn't dectect simple trojans like siteno! By the time I noticed real problems it was too late!
Time to grab the copy of Microscope-2000, here comes the Low Level Format, followed by da Penguin and a Debian Format just to be extra sure. Last 2 days were spent screwtinizing and scanning EVERY SINGLE THING that went back into the machine. Renguard being the LAST thing I did, went and installed HKEY_Local_Machine\System\ControllSet Legacy entries for svkp ALL OVER THE PLACE! Rerouted my image path, ect.....

There is NO SAFE way I can find to GET RID OF THEM ONCE THEY ARE THERE! I can't delete the strings, values, and/or keys, I can't modify them, I can't modify the binary data. The ONLY thing I could do was take ownership of them!! This crippled the graphics of the machine! Caused the device manager's settings to DISAPPEAR!
NO JOKE! I go to open up the device manager to see what is going on with the drivers ect.. and I'm looking at a BLANK window!?!?

Some security sites list svkp as a hack-tool/root-kit, others list it as W32/Spybot, and Cert.org of all people don't have anything about it on their site about it?!?

The spyware scanners ALL list it as a medium to medium high level threat after scanning. Some network admins have told me to "Beware of this program" forms of it are known to infect computers threw IRC, were it can wait for commands from remote hosts.

If I'm going to keep running renguard, it will probably be from behind a HARDWARE Firewall Running EnJoy 3 with DEEP Packet filtration