Subject: Re: Renguard/Norton Problems
Posted by Blazer on Sat, 22 Oct 2005 18:49:06 GMT
View Forum Message <> Reply to Message

HTGunny wrote on Sat, 22 October 2005 12:27ok if i am readin this correctly - norton is causin this hacktool thing thru svkp - an ya'all are suggestin that we allow it by forcin nortons to ignore it - hmm
Yes.

HTGunny wrote on Sat, 22 October 2005 12:27
now my question is - what about the actual viruses or worms or what ever that are usin svkp - if we allow it then we might as well as throw all our anti virus programs away and let the infections begain
Norton is detecting svkp.sys as "Hacktool.rootkit", which is just a generic classification of "we think this is a tool that hackers might use". It is more of an informational/caution message than an actual virus hit. What I mean to say is, by telling Norton to ignore svkp.sys, you are not making yourself vulnerable to viruses or trojans that use svkp, because Norton would fingerprint that specific virus, and there would be a special definitition for it like "rootkit.w32SomeTrojan". Antivirus scanners mostly work off of "fingerprints", which are CRC/checksums of parts of files. If a real virus was released that used svkp, Norton would not rely on just finding svkp.sys to detect it, it would have a fingerprint of the main virus executable itself, so you would still be protected.

HTGunny wrote on Sat, 22 October 2005 12:27
so what am i supposed to do

i wont throw my antivirus away nor will i force it to allow svkp. this seams like a problem that you guys need to address and repair versus puttin your hands over your eyes and sayin to ignore it
It depends on if you want to be a sheep and go along with Nortons idiotic claim that anything that uses SVKP is bad. That's like saying a C compiler is bad, because virus and trojans are compiled with one "Detected Microsoft Visual Studio.Hacktool.rootkit!". We paid money to license SVKP because it's the best at what it does. If we use some other protection, who is to say that Norton won't add it too (and maybe already has). I think its easy to see that Symantec/Norton are the ones who have overstepped their bounds here, and while I would like to think that we could talk to their support people and have the definition removed, I doubt it, so that means the only course of action that can be taken is by you

HTGunny wrote on Sat, 22 October 2005 12:27i trust your program - its a pain at times but very functional and i commend you all on it - but i am forced to not use RG till YOU fix it As I said, there is nothing *we* can fix. The only way that we could try to fix it, is to not use SVKP, or any other sort of protection in the next version of RenGuard. Sadly, if we did that, RenGuard would get hacked in about 30 seconds from release. I don't really have time to explain in detail, but suffice to say that RenGuard without SVKP or something similar, would be like RenGuard being a renguard.txt, with one line that says "hacked=false", that someone could just edit to say "hacked=true".

HTGunny wrote on Sat, 22 October 2005 12:27
bummer too - i really liked it

thanks alot for everything and good luck on this one

I understand your frustration and believe me, nobody is more frustrated than us. We will continue to try to find the easiest solution, but in the meantime we recommend making Norton ignore svkp.sys. We would not make this recommendation if we thought it would expose your PC to other harms.