Subject: Re: Renguard/Norton Problems
Posted by Blazer on Mon, 24 Oct 2005 12:00:40 GMT
View Forum Message <> Reply to Message

ingram091 wrote on Mon, 24 October 2005 06:52
My problem is not with your using the tool, its not taking action to eliminate the need for a tool that is being used by numerous worms and viruses out there to launch their attacks. AND telling people to just allow it to work ignoring the virus warning.

Firstly, we cannot "eliminate the need for" the tool. If RG is not encrypted, there would be cracked copies of it out within 24 hours, and people would even be poking around it with a hex editor. And I would like to point out, that there has been no "virus warning". The alert the Symantec/Norton gives, if you actually take the time to read it, is that svkp.sys is not a virus itself, but rather may be part of or indication of another virus or trojan. To be honest, I have never heard or actually seen SVKP used for an actual virus, most script kiddies use UPX and other free exe wrappers.

ingram091 wrote on Mon, 24 October 2005 06:52
New viruses are NOT caught in time by anti-virus companies all the time. So by white listing a blocked tool you put yourself at a higher risk then is recommended. Just to use your program. As I said, blacklisting SVKP is about as silly as blacklisting Visual C++, since afterall, they can both be used to create or part of a virus. If its possible, I would recommend some combination of settings such that svkp.sys is ignored, except if something tries to overwrite it.

ingram091 wrote on Mon, 24 October 2005 06:52
According to a message I received from AntiCracking@AntiCracking.sk the golden support customer base are able to receive an updated method for embedding their protection into their compiled executable. all you have to do is request a support ticket on the matter.
SVKP is a kernel mode ring-0 driver, and you cannot simply embed it into an executable. They do have lesser forms of protection that are not ring0 and can be embedded, but they can also be bypassed with ease, which is why we use the more elaborate solution.

ingram091 wrote on Mon, 24 October 2005 06:52
This is a computer safety issue, not a renguard issue.
according to symantec here http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.ubh.html the file "Creates the file %System%\SVKP.sys. This is used by the worm to unpack itself and execute" this is one of many worms currently using this method. Thats is why all of them are now adding it to their list of blocked signatures.

That particular worm not only creates an SVKP.sys, it also exploits a bug in windows PNP (which has long since been fixed), and connects to an irc network. For to get infected by that worm, they would have to have a non-updated windows installation, the virus infection, and no firewall whatsoever (or at least one that wouldnt stop or popup on the outgoing irc connection). If they meet any of those criteria, I doubt blacklisting svkp will make them any more secure

ingram091 wrote on Mon, 24 October 2005 06:52
Thus it is a vulnerability that should not be used if at all possible. the developers are aware of its current abuse and are taking stems to secure the method through other means. but at this time its a vulnerability, most. including myself, are not willing to risk using just for a 3rd party

anti-cheating program.

Until I hear of a significant number of cases where an actual virus uses SVKP, I would not be concerned at all about whitelisting SVKP.sys. The very URL you provided as "proof", shows that the number of reported infections were "0-49"...I bet it was a lot closer to 0 (like a single report), than it was to 49.

Despite my views, I do recognize that it's your computer and you are entitled to be a paranoid as you want. Just know that we are very aware of the issue and are taking steps to do what we can, including considering a different protection software for RG 1.04, and accelerating the development of RG 1.04.