Subject: Renguard not connecting; Worm threat occurs simultaneously
Posted by Beta on Sat, 23 Sep 2006 23:47:48 GMT
View Forum Message <> Reply to Message

Just tried firing up Renegade and Renguard for the first time in almost a year. Didn't work. Went through a few checks, then one of my spyware scanners gave me a worm message, then Renguard gave me an error.

The program which gave me the warning is STOPzilla. The name of the worm is Surila.B. Is it related to this? If so, what do I do... just allow it?

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by light on Sun, 24 Sep 2006 01:57:50 GMT
View Forum Message <> Reply to Message

Yes, I believe it's a false positive.

Quote:W32/Surila-B is a network worm which may try to send a link to itself or W32/MyDoom-W to ICQ contacts.

W32/Surila-B places the main component of itself as dx32cxlp.exe to the Windows system folder and the All Users' startup folder, and as systemst.exe to the Windows system folder. The worm also drops other components of itself to iexpl1orer.exe and SVKP.sys in the Windows system folder.

W32/Surila-B creates the following registry entry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
iestart = <path to iexp1orer.exe>

Additionally W32/Surila-B creates a service named SVKP which causes the file SVKP.sys to be executed when the service starts, for example at system startup.
http://www.sophos.com/virusinfo/analyses/w32surilab.html

Renguard uses SVKP.sys for protection against is being decompiled by cheater (IIRC). SVKP.sys is not a danger to your system.

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by 0x90 on Sun, 24 Sep 2006 11:35:16 GMT
View Forum Message <> Reply to Message

light wrote on Sun, 24 September 2006 03:57
Renguard uses SVKP.sys for protection against is being decompiled by cheater (IIRC). SVKP.sys is not a danger to your system.

yeah lol.. and it does it very well.... (not)

i really dont know - since so many honest RG players have problems with svkp and since its fully 'hacked' and therefore worthless - why they dont release a non-packed RenGuard version.
perhaps the 64bit os problem will be solved with this also.
3rd party exe packers almost always cause unpredictable problems.

just my 2cents.
0x90

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by cmatt42 on Sun, 24 Sep 2006 14:24:57 GMT
View Forum Message <> Reply to Message

0x90 wrote on Sun, 24 September 2006 06:35

yeah lol.. and it does it very well.... (not)

i really dont know - since so many honest RG players have problems with svkp and since its fully 'hacked' and therefore worthless - why they dont release a non-packed RenGuard version.
perhaps the 64bit os problem will be solved with this also.
3rd party exe packers almost always cause unpredictable problems.

just my 2cents.
0x90
Hey, guess what? All of these problems will/have already been solved for the next version!

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by 0x90 on Sun, 24 Sep 2006 14:56:40 GMT
View Forum Message <> Reply to Message

cmatt42 wrote on Sun, 24 September 2006 16:24
Hey, guess what? All of these problems will/have already been solved for the next version!

ahh sorry, of course! stupid me! the high&mighty next version of renguard! the holy 1.04! when will it be released again? soon? or next wednesday?
hey.. you could always make an anticheat for duke nukem forever! THAT would be great

0x90

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by Blazer on Sun, 24 Sep 2006 15:59:12 GMT
View Forum Message <> Reply to Message

The next version does solve it, and doesn't use SVKP.

Subject: Re: Renguard not connecting; Worm threat occurs simultaneously
Posted by Goztow on Mon, 25 Sep 2006 07:03:53 GMT
View Forum Message <> Reply to Message

If it wasn't for people like 0x90, it wouldn't have needed this protection at the first place, right?