

Re: Unable to boot after using regrun/unhackme/partizan, whatever.

## Re: Unable to boot after using regrun/unhackme/partizan, whatever.

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2008-03/msg02070.htm](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2008-03/msg02070.htm)

---

- *From:* "Mark L. Ferguson" <[MarkLFerguson@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:MarkLFerguson@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 28 Mar 2008 16:55:19 -0500
- 

How to Recover from a Corrupted Registry –config–system:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q307545>

--

Was this helpful? Then click the Ratings button. Voting helps the web interface. [http://www.microsoft.com/wn3/locales/help/help\\_en-us.htm#RateAPostAsAnswer](http://www.microsoft.com/wn3/locales/help/help_en-us.htm#RateAPostAsAnswer)

Mark L. Ferguson

..

"necrophyte" <[necrophyte@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:necrophyte@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message <news:F1CB7471-BFDD-42F6-8B5B-D51D17829776@xxxxxxxxxxxxxxxxxxxxx>

well, i'm sure autoruns would help me, if i was able to start it anyhow – but i am not. i cannot get windows to boot – in neither mode, and while using the recovery console with my OS cd i cannot eject the cd and insert another one on which i'd burned autoruns. (my notebook has no floppy drive)

i have an external HD connected over usb – but while in the recovery console it is not being recognized – which drivers/controllers etc. should i load while in the recovery console in order to be able to use the external usb HD?

thanks

"Mark L. Ferguson" wrote:

AutoRuns for Windows v8.61:

<http://www.microsoft.com/technet/sysinternals/SystemInformation/Autoruns.msp>

--

Was this helpful? Then click the Ratings button. Voting helps the web interface.

[http://www.microsoft.com/wn3/locales/help/help\\_en-us.htm#RateAPostAsAnswer](http://www.microsoft.com/wn3/locales/help/help_en-us.htm#RateAPostAsAnswer)

Mark L. Ferguson

.

"necrophyte" <[necrophyte@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:necrophyte@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in

Re: Unable to boot after using regrun/unhackme/partizan, whatever.

message

news:F1DC9094-94CE-4329-8D3A-D95DD6FBA21F@xxxxxxxxxxxxxxxxxxxx

> this is what i already posted on tech-forums.net:

>

> still banging head against a wall that i even installed that #\*%&

> software... this is what i already posted in the support forum of that

> software's company's website (www.greatis.com):

>

> i just installed regrun platinum 5.7 since i read that this software > was

> able to remove win32/iroffer, which i suspected to have some remaining,

> non-active files left on my computer (ms-java.exe, s.dll etc.), which > it

> by

> the way did not although present in the windows/driver/i386 folder..

>

> i updated the database, ran some utilities (didnt delete anything, just

> looked at what it would detect – as mentioned before, it didnt detect

> ms-java.exe as a malware..), and then ran the partizan bootwatch > rootkit

> detection which asked me to reboot in order to search for rootkits...

>

> i did so, and after the winxp bootscreen a blue screen appeared saying

>

> regrun partizan – bootwatch antirootkit. greatis software (c) 2007–2008

> partizan driver is active.

>

> well, thats as far as my computer comes now. safe mode > hangs up while

> still booting up windows (last loaded device is mup.sys)

>

> last good configuration causes blank screen.

>

> CTRL-ALT-DEL doesnt work. i can only boot again after shutting down

> using

> the power button.

>

>

> i. e. – OBVIOUSLY NO WAY TO BOOT MY COMPUTER AGAIN

>

> any suggestions?

>

> i can 100% assure that my computer was completely >

> spyware/malware/virus–

> FREE

>

> specs:

> hp notebook nx9030

> winxp professional sp2

>

> before rebooting after running regrun/partizan.. for the first time,

> EVERYTHING WENT PERFECTLY

>

>

> any suggestions?

Re: Unable to boot after using regrun/unhackme/partizan, whatever.

> PS: debugging mode – same problem, win domain controllers only – after  
> loading controllers the partizan driver is active text appears again, > but  
> this time on the black screen, not the win blue screen.  
>  
> -----  
>  
> i just disabled "partizan" using bootcfg in the recovery console.  
>  
> well, now after the windows bootscreen the same blue screen appears, >  
> only  
> now it only says:  
>  
> regrun partizan – bootwatch antirootkit. gratis software (c) 2007–2008  
>  
>  
> without "partizan driver is active."  
>  
> i cant find any other service that is still enabled that could be part > of  
> that software.  
>  
> is there any other way to disable everything related to that  
> regrun/unhackme/partizan trash? it has to be started before all other  
> services in order to detect rootkits, so where could that entry be, > maybe  
> registry? can i access the registry somehow?  
>  
> i still cant believe this is happening.. some few hours ago my computer  
> went  
> perfectly and now..  
>  
> -----  
>  
> i just found some technical information about that trash..  
>  
> partizan (part of unhackme, which is part of the regrun suite :/) > starts  
> using the UNHACKMEDRV.SYS kernel driver  
>  
> in the registry the entries are  
> HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Contro  
l\Session Manager  
> BootExecute  
>  
> and RunOnceEx  
>  
>  
> ..so, anyone an idea how to stop/disable/delete/reset UNHACKME.SYS  
> and  
> those  
> two registry entries (bootexecute & runonceex) using the recovery >  
> console  
> or  
> any other method while not being able to boot windows?

Re: Unable to boot after using regrun/unhackme/partizan, whatever.

>  
> thanks..