

Final Report Vundo

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.configuration_manage/2008-01/msg00085

- *From:* "stand_58" <exray@xxxxxxxxxxx>
 - *Date:* Sat, 26 Jan 2008 19:28:59 -0500
-

Mr. Green, you led me to a place from which I could get rid of this bugger.

The heavy lifting was the work done by Shedrick in the posting you pointed me at in the forum, and the major path to fixing was the files pointed to by the Run key in the registry that got renamed to have a space before the .exe, and then had a bunch of crap added to them. Just looking for those and systematically getting rid of the larger versions of them, renaming each of the diddled * .exe files to *MUSTFIX.exe, and finally getting rid of all the garbage created in windows\system32, took away a lot of the engine from this miserable load of bits.

Since I have a dual boot capability (media center and xp), there's nothing in the infected partition that is undeletable, though of course editing the registry is more easily done from the XP partition.

After I used Media Center to do the editing in the XP partition, I booted into XP and was able to take advantage of the load= line being filled up by Vundo with a now deleted file (another thing that Shedrick explained in his posting) and do the same kind of registry cleaning Shedrick did.

Amazingly, I didn't even need to use the tools or Hijackthis. The Vundo variant that I had wasn't quite as determined in keeping itself going as it first seemed....its creators could have made it even more of a trial to restore a machine to good order.

So finally, again, thank you Mr. Green (directly) and Shedrick (by proxy)

"V Green" <vanceg@xxxxxxxxxxx> wrote in message
[news:uzk\\$MOUXIHA.5364@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](news:uzk$MOUXIHA.5364@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

OK, great.

Basically what remember doing (was a while ago) was to kill all bogus processes with Task Manager. Then look for suspect entries with the same name in the Registry and delete those.

Then look for recently created files with nonsense names in the usual places in \WINDOWS and \Documents and Settings.

Final Report Vundo

If they won't delete in regular or Safe Mode, write a script in Notepad with the pathname of the files that you want to delete that are locked, example:

C:\Windows\system32\khffddc.dll

Save this to your desktop as vundofix.vft – type "All Files".

Then start VundoFix and drag vundofix.vft onto it. Click the Remove Vundo button.

VundoFix will "unlock" the files and delete them. Screen may go blank and you might have to reboot.

Run HijackThis and look for anything else (you can use HJT to take the place of the manual Registry search above – it found all the same entries that took me much longer to find with Search).

Good luck. It is possible to beat this sumbitch.

"stand_58" <stand_58@xxxxxxxxxxxx> wrote in message
news:%23pxXUGUXIHA.4440@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Mr. G. Thank you so very much for your reply. I've tried the tool, it's really good....and ultimately it didn't do the job.

But the article you pointed out is amazingly good. Shedrick really has teased out all the issues that likely beset my machine, and better than that he intelligently walked the paths that I found myself blindly stumbling around in when I spent a day failing to bet this bugger.

If I find anything different from what he found, I'll post it. (my junk is called ddayv.dll and ddayv.exe, and I also get vyadd.ini readily created. Other than that.....I have to print out his article and follow his lead.

And again, thanks to you.
"V Green" <vanceg@xxxxxxxxxxxx> wrote in message
news:uGaR1HLXIHA.4140@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

<http://vundofix.atribune.org/>

Try the tool. For me it got most of it, but I had to manually remove a bogus .DLL (see the forums on how to do this—drag n' drop a vundofix.vft file onto vundofix after stopping all processes related to it).

Final Report Vundo

HijackThis is also needed to tell you where the SOB is hiding in the Registry. If you know what you're doing, you won't need to send the log to anyone, just interpret it yourself. You already know what you're looking for.

You might like this forum entry:

<http://www.atribune.org/forums/index.php?showtopic=3660>

BTW, I got infected through an exploitable version of the Sun Java Runtime after running one of those applets that Ebay uses to show pictures of an item.

"stand_58" <stand_58@xxxxxxxxxxxx> wrote in message news:Onj8kt7WIHA.748@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Not the ordinary question, though.

I have a dual boot system; media center edition is not blessed with this miserable trojan/virus/worm, while my XPSP2 is. I use XP as the default, and of course years of using it means it's set up the way I want it, and I don't want to just trash it or bear the consequence of what a repair install might do to me, especially since I don't have SP2 slipstreamed into my original XP disk.

Anyway, what I have done is to try using some of the VUNDO trojan removal tools. The flavor of Vundo that I have keeps on producing files like ddayv.exe and ddayv.dll in the system32 directory, and running them. Also vyadd.ini files in that directory. It shovels load instructions for the ddayv.exe into the registry in a few places.

I can edit the registry and get rid of all the junk that I find, but

Final Report Vundo

of course I'm not finding the root of the problem. I can also boot into the media center and use that to edit the xp windows\system32 directory and get rid of all the files created in there since the virus hit.

I can work in safe mode in XP and the trojan doesn't write all the garbage that it typically writes.

Now here's something interesting.

I'll have gotten rid of all the instances of ddayv.exe, and then I'll boot. I get a message box that looks as if I've tried to open ddayv.exe and windows\system32 just can't find it, and if I want to search for it (yeah, right) I can do so. The system tray has not yet loaded, the GUI is up, Windows is usable, but ddayv.exe has not yet been created in the system32 directory.

I just click OK on the message box, the boot process continues, and the new garbage gets written into the registry and into the system32 folder.

The help I am looking for from you people is some kind of utility that will let me step through the end of the boot process. I know there's a step by step way of doing a cold boot and a bootlog can be captured (am I only living in the Win 98 world

Final Report Vundo

here?...remembering a capability long gone?).
The question is whether there is something available that would let me walk through the later stages of the boot process so I can find out just what it is that first invokes rundll to make the ddayv.dll run....and before that, what makes ddayv.exe create ddayv.dll, and before that what makes ddayv.exe get created from apparently nothing. There's got to be a way to drill down to that nothing.

So this is a long post, I hope I'm not asking the impossible and I'm not looking to post a hijack this log so somebody can create a batch file for me or recommend a list of steps to take.

Thanks in advance.