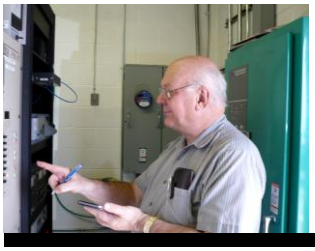

The
Broadcasters' Desktop Resource
www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Doing IT Right

Getting Rid of the Vundo Trojan Virus

by Paul Litwinovich

[December 2009] Keeping computers free from some of the nasty stuff on the Internet requires constant vigilance, perhaps with an anti-malware program. Computers used by the staff in the Control Room are even more vulnerable, as users may use less care when on such commonly shared computers. If your facility gets "got," Paul Litwinovich has the solution:

I manage about 70 computers here at the WSHU Public Radio Group and have gotten quite good at cleaning up the occasional virus that usually slips by in someone's e-mail.

In recent weeks, there has been a rash of new computer infections caused by the Vundo Trojan and its viral variants. This was an exceptionally tough one, so I had to do quite a bit of research on it. Perhaps this information will alert you to the dangers – and help if you find it on your computer.

INFECTION BY TROJAN

The infection can occur easily: the Vundo Trojan starts as a pop up in your web browser telling the user that the computer's antivirus program is about to expire – or has. It asks you to "click here to fix the problem." It may offer a free download of "Internet Security 2010" or some other program to "clean your computer."

WARNING: if you or your staff see this pop up, ***do not be tempted to click the "X" to close the box.*** It is all one jpeg and ***if you click anywhere on it, it will begin the download process.*** On some variants you can right click the icon for your browser in the lower task bar at the bottom of your screen and close the browser. If you are lucky, this will also close the pop up.

If the pop up remains on your screen at this point, the only way out is to save any open files (documents, etc., that you were working on) and then *crash the computer* by holding down the power switch until it shuts down. You may have to go through a disk check when you reboot, but it beats the alternative.

Warning: Doing a normal, clean shutdown will give it a chance to write itself to your hard drive.

WHAT VUNDO DOES

There are many variations of the Vundo Trojans, ranging from the "relatively" benign to the very destructive. Most use the appearance of some sort of pop-up advertising and then root themselves to make them difficult to delete.

If you click on the pop up, it will fool some anti-virus programs by appearing as an intentional download.

Then, once the virus has loaded itself, it will attempt to shut off your real anti-virus program and replace its icon in your system tray with one for a bogus anti-virus program. It can modify your security settings to display a warning that your anti-virus program needs to be updated and when you click on the warning it will take you to a bogus website and attempt to sell you more fake software, or at least get your credit card number. The fake anti-virus program can appear under a number of names.

The virus will often switch off automatic updates, and create a file that prevents you from starting in the safe mode. It will often write protect a copy of itself in the browser cache which can not be removed. If the virus detects that you are trying to remove it, it can create dozens of copies of itself appearing as weird named dll files in the system32 directory. More details of how Vundo works are available on most anti-virus web sites.

One point that can be found on almost all web descriptions of Vundo is that it flings wide the gates to let other Trojans in, so the longer your computer is untreated, the more viruses you will have to deal with. Fortunately, these will clean up easily when you scan the drive after making the changes to remove Vundo.

Additionally, it may even "invite" other viruses to come take residence: You will often get pop up ads for other websites, products, and porn, in addition to ads for the bogus anti-virus program.

ANALYSIS

The key is the way it stores a copy of itself in the hidden system volume information folder (which is used to store restore points), write-protected with all but system access denied – so your real antivirus (if still functional) or online scans like Trend Housecall cannot always remove it. It is also very good at preventing removal tools from loading and executing.

In fact, AVG, Trend, and Norton would all detect it and think that they were removing it, but there it remained. I discovered this when I tried to scan only the SVI folder and *found no change in its size* after the anti-virus reported cleaning the virus. I then found that the virus files were pretty much locked down.

HOW TO RECOVER FROM VUNDO

It is very hard – in fact, almost impossible – to get rid of this virus from the infected machine itself.

The only sure way to clean up this infection is use one of those adapters that let you plug a hard drive into a USB port such as the Olevia ADA-2020 or similar.

Here is how to clean up your computer:

1. Remove the infected drive from its machine.
2. Connect it to the USB adapter plugged into a machine with an up-to-date anti-virus program.
3. Cancel the annoying autoplay program that Windows opens when it sees the drive.
4. Open the drive within Windows. (Do not worry: this type of virus cannot infect the other computer while doing this, it can only operate from the C: drive)
5. Once the drive is open and you can see its contents, from the explorer tool bar open: tools/folder options/view and check "show hidden files," then uncheck "hide protected operating system files."
6. You will now see the system volume information folder. Right click it and under properties uncheck "read only." While still in properties, go to the security tab and add the current user or administrator as having "full control" (the default system user is not enough). Make sure you apply this setting to subfolders (i.e., if you log in as “Joe” add “Joe” to the allowed users for the drive that you are repairing).
7. Close the properties box and now click on the folder to see if it opens and you can see the files.
8. Close Windows explorer.
9. Click my computer, then right click the infected drive and select "scan with (whatever) antivirus" you use. Make sure you tell the program to *remove* all detected threats. (If using AVG Free, make sure that you are up to version 9, as 8.5 will not remove all of these viruses.)
10. After the drive is clean, put it back in its original machine.
11. When it starts, you may get the message that it cannot find this or that file or .dll, etc. This is *not* an indication that the machine is still infected. The registry is looking for files created by the virus that are now removed. Note what the files are and then use regedit to find the lines calling for them and delete these registry entries.

If all goes well, you should now be able to reboot the machine and get a clean boot. You may have to turn automatic updates back on, but otherwise I have not found any permanent damage.

After altering the property settings as described, I was able to clean the whole disc in one shot. I have since used this method to clean the infection from several other computers so I have a high level of confidence in the method.

I hope this helps you, if you find yourself facing this annoying menace.

- - -

Paul Litwinovich is the Director of Engineering for WSHU AM&FM and WSUF-FM in Fairfield, CT. Contact him at paull@wshu.org

Return to The BDR Menu