

# Salvaging your system after a malware infestation



John Deans

To wrap up our three part series on malware, let's review what we have learned over the past couple of weeks.

Number one, malware infestations are getting more frequent and becoming less benign. Last week we talked about ways to

avoid getting hit with spyware and Trojans by staying away from certain websites and not typing specific keywords into search engines.

Malware infestations can be brought in from your kids looking for free stuff on the Internet or you going to funky sites other than mainstream web pages. If you have not been able to avoid getting slammed by malware and your PC is in a world of hurt, there are a few last ditch efforts you can try to salvage your computer.

These are extreme measures and they should only be initiated if regular scans by your antivirus and antispayware software have failed to remove the digital gremlins.

Before we even go down this road, make sure you back up your data. Do this with an external hard drive, CDRom, thumb drives, or remote backup ser-

vice like Mozy.com, DataDepositBox.com or Carbonite.com.

First we'll start off easy and use SpyBot to make the first pass of detoxifying your computer. Google Spybot, click on the link by Safer-Net-working.org, and then download and install

the latest version which should be 1.6.2. Refer to my previous article for more detailed instructions on Spybot at [www.DeansConsulting.com](http://www.DeansConsulting.com).

The difference here is that you are going to execute the Search and Destroy phase in Safe Mode of Windows. This enables Spybot to do a more thorough job of eliminating malware because not all the negative processes have had a chance to start up in Safe Mode.

Just after powering up your computer get ready to hit the F8 function key immediately after you see the computer vendor POST (Power On Self Test) message but before Windows starts up. After that you will have a choice of start-up options and you will want to pick Safe Mode with Networking.

Now that the computer is basically half way up and partially functional you will start up

SpyBot and begin the Check For Problems button. Let it run to completion and then hit the Fix All Problems after the search has completed.

If it asks you to reboot for it to scan a second time during boot up then let it. After all the problems have been fixed, reboot the PC yet again but let it come up in full operation mode.

If you are still having problems, start up MScONFIG by clicking on Start-Run and typing the command "msconfig" at the open or command line. From there click on the Service tab and then check the box of "Hide All Microsoft Services" to keep you from turning off a critical service that Windows needs.

Here under the services tab you can turn off all services other than the antivirus software. Remember, you are not removing software but rather just temporarily disabling it.

The goal here is to turn off some bad stuff so the antivirus and antispayware can knock it out.

Malware can be very tricky because once it gets started it first tries to hide itself so you cannot find it to eliminate it. Some malware even disables the antivirus and antispayware applications. The really pain-in-the-tail ones have the audacity to disable MScONFIG and Task Manager.

Also in MScONFIG is the Startup tab with the processes that startup after the services. Do the same thing by disabling all the startup items except for the antivirus software.

Then hit OK and let the com-

puter reboot. After it comes up it will warn you that items have been blocked from starting up but you can disable that warning message by checking the little box on the lower left.

Run Spybot again after the cleaner system has rebooted and give it a chance to knock out more bad entities. If that does not work, you may have to resort to the big gun called ComboFix.

Google ComboFix, download it from [BleepingComputer.com](http://BleepingComputer.com), and start the installation process. It will beep loudly a couple of times and warn you that it is a dangerous last resort anti-malware application, but be brave. Let it create a restore point, backup the Window's registry, and even install the Microsoft Windows Recovery Console just in case things go bad.

After all the preparation processes have completed, you will then see an old fashion blue DOS screen appear and the stages of cleaning will begin. ComboFix may even reboot the computer a couple of times and restart the stages so do not interrupt it or get too worried about it. Let it completely finish until you see a white screen with black text which is the log file appearing as the final step.

From there you can reboot the computer a final time and try things out to see if any improvements to system performance and stability have been made. ComboFix has repaired numerous systems over the past two years and has kept me from completely rebuilding them.

If none of these procedures

helps get your computer out of malware hell then it may be time to hand it over to Computer Helpers and let them have a crack at it. They have accumulated and tested dozens of anti-malware utilities that they use in series based on the unique behaviors that critically infected computers reveal.

Since one guy can troubleshoot numerous systems at simultaneously, Harper and his crew are set up very well for

malware battles.

Bottom line: After you learn about malware and utilize ways to avoid it, hopefully you'll never have to use these harsh techniques to fight those little buggers.

Next week's column: Limiting screen time.

*John Deans of DeansConsulting.com is a Brenham area computer networking consultant who can be reached at 289-2233 or [John@DeansConsulting.com](mailto:John@DeansConsulting.com) for questions and comments.*