



## TECHNOLOGY INSIGHTS

### How to Clean Up a Serious Malware Infection

They say it can happen to anyone. Late last year, it happened to the Editor in Chief at mega-tech website ZDNet <http://blogs.zdnet.com/BTL/?p=27234&tag=nl.e539> . You'd think someone of Larry Dignan's experience would know how to handle the clean-up, or call on one of the security gurus at ZDNet. Not so. Larry doesn't even mention Safe Mode. Strange. Here's the rough guide, should you ever need it:

#### 1. Download a Smart Online Scanner

It's not much use running a scan with the internet security suite on the infected PC, since it missed the intrusion in the first place. As it happens, most AV-software companies now have malware scanners they let you access online or download for free. The difference lies in how much malware they find, how well they clean up, and how heavy-handed they get in collecting their ransom. Some will get rid of a few infections, then hold a gun to your head demanding you buy their software before they finish the job. Not very subtle, but that's the security mafia for you.

Others won't run with Firefox if that's your browser of choice, and others again just drown you in advertising. ESET does none of these things and offers its highly regarded NOD32 scanner without attaching strings made of piano wire. It will clean up most of what it finds, and all you have to do is press the OK button. Here's the download link [www.eset.com/onlinescan/](http://www.eset.com/onlinescan/)

Use ESET's Online Antivirus Scan and Make Sure Your System Is Clean

### ESET Online Scanner

#### ESET Online Scanner

ESET Online Scanner is a user friendly, free and powerful tool which you can use to remove malware from any PC utilizing only your web browser without having to install anti-virus software. ESET Online Scanner uses the same ThreatSense® technology and signatures as ESET Smart Security/ESET NOD32 Antivirus, and is always up-to-date.

**IMPORTANT:** Administrator privileges are required to run ESET Online Scanner

ESET Online Scanner

[Scanner](#) | [New Features](#) | [Benefits](#) | [System Requirements](#) | [Help](#) | [FAQ](#)

If you don't like the ESET scanner, other good options are Bitdefender's online scanner <http://www.bitdefender.com/scanner/online/free.html> and Avast's virus cleaner which you can grab here: <http://www.avast.com/eng/avast-virus-cleaner.html>

#### 2. What if the PC keeps crashing?

PCs can become so infested that malware scans cause crashes, or the scans won't run reliably or the software won't install. If that happens, the first option is to reboot the PC in Safe Mode with Networking. You get there by tapping F8 when you reboot the PC. Some PCs use a different function – you may need to check the manual. Safe Mode in Windows starts only the most essential processes, and you can choose the additional ones you want to use. Safe Mode should be easier to run online scans or install cleaning software. Why Larry from ZDNet didn't try this is anyone's guess.

These are our own opinions.

We have no commercial arrangements with vendors.

For more reviews, please contact TECHNOLEDGE.

T +61 2 9909 0246  
E [info@technoledge.com.au](mailto:info@technoledge.com.au)  
W [www.technoledge.com.au](http://www.technoledge.com.au)

### 3. Radical rescue

If you're still having problems, Avira offers a free rescue disk that lets you boot into your PC and run the scan and use the repair tools provided without booting into Windows. This disk also works without connection to the internet so you can fully isolate the PC and stop any spyware hiding inside from calling home. (Of course, it helps to have a second PC handy for downloading some of these tools).

Here's the link [http://www.avira.com/en/support/support\\_downloads.html](http://www.avira.com/en/support/support_downloads.html)

This isn't option for the faint-hearted but here's a guide that'll make the job easier <http://forum.avira.com/wbb/index.php?page=Thread&threadID=8216>

Like Eset, Avira is another trusted name you probably haven't heard of. The download is about 60mb and needs to be burnt to disk in ISO format. If your burner doesn't burn ISO disks, Ashampoo's free Burning Studio is a good choice. You can find it here: [http://download.cnet.com/Ashampoo-Burning-Studio-Free/3000-2646\\_4-10776287.html](http://download.cnet.com/Ashampoo-Burning-Studio-Free/3000-2646_4-10776287.html)

### 4. Play it again, Sam

If infections are numerous or severe, it will take more than one attempt and more than one scanner to clean up properly. And certain kinds of spyware can be hard to track down and prize out, Trojans and rootkits for example. You can use programs like Webroot's Spysweeper, Malware-Bytes or PC Tools Spyware Doctor – none of these offer online scans and all will put the hard word on you.

An easier option is Threatfire, the free Intrusion Protection program from PC Tools and a long favourite of ours. It does a good job dealing with spyware. <http://www.threatfire.com/?qclid=COntu56f9Z0CFSn6agodIilNIw>

Another free but effective option is SuperAntiSpyware. A more comprehensive malware removal resource for the more technically savvy can be found here <http://www.techsupportalert.com/content/spyware-removal-guide.htm>

### 5. Patience is a virtue

A thorough clean-up with multiple tools takes time and patience. Wiping the disk and re-installing everything may look attractive at some point, but don't be too hasty - chances are that your recent backups are infected as well.

And if you think Windows' System Restore points will set the clock back to a malware-free past, think again: system restore only effects changes to the Windows Registry. Any programs you've installed since the restore point will be disabled, but all the files they've infected are still on your system.

### 6. An ounce of Prevention beats a ton of cure

To prevent future infection, make sure you have two layers of protection installed and keep those update. The first layer should be a traditional internet security suite with AV engine, firewall, spam filter and so on, the second should be an intrusion prevention system like PREVX3. If the cost is an issue, go with Avast Home (free) and Threatfire.

<http://www.avast.com/eng/download-avast-home.html>

Also, make sure you install Windows updates whenever that yellow symbol appears in your notification area (bottom right of the tool bar). And once in a while, run Secunia's online scanner to make sure that all your important software has the latest patches applied.

[http://secunia.com/vulnerability\\_scanning/online/](http://secunia.com/vulnerability_scanning/online/)

# # #