



## TECHNOLOGY INSIGHTS

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)

## Driver Training

### A survival guide for the internet highway

#### PART 3 - AFTER AN ACCIDENT

#### It can happen to any of us

No matter how many layers of security you have in place, you can get infected. Zero-day threats are the hardest for AV engines to cope with, since they lean heavily on databases of existing fingerprints. Good AVs employ heuristic techniques as well as signature-based detection, which enables them to spot new malware types by their suspect behaviour rather than their fingerprints.

Heuristic detection is not yet as effective as fingerprinting. ESET's **NOD32** relies heavily on heuristics and has the best record for detecting zero-day threats, but even it only catches some 70%. The percentage improves if you add other security shields like Host Intrusion Protection Systems (HIPS), but 100% protection is only possible by getting off the internet highway altogether.

#### Tools of the Trade

If your PC develops bad habits and you've ruled out hardware and software gremlins, a number of tools are on offer for tracking down and removing uninvited guests. Since the malware got past your existing defences, it's best to use detection tools from another source.

ESET has a reputation for finding malware other AV programs miss. The company makes an online scanner that runs across your system, gives you a report and cleans up if you ask it to. It is almost free of the advertising other online scanners hit you with during the operation - <http://www.eset.com/onlinescan/>

*Trend Micro's HouseCall* <http://housecall.trendmicro.com/> is loaded with ads for PC-Cillin but at least it will clean up what it finds unlike Norton, McAfee and Kaspersky whose scanners only tell you what they found. Then they suggest you buy their products right away to get rid of the offending malware. That's called gun-to-the-head marketing.

*Trend Micro* also makes a **CWS Shredder**. It removes 'Cool Web Search', a euphemism for a range of browser hijackers - <http://www.trendmicro.com/cwshredder/>

Microsoft's **Malicious Software Removal Tool** comes down the line about once a month, whether you want it or not, usually with Windows Updates. It's hard to tell what it does or what it finds—I've never seen a report from it or even a message.

If the these tools don't shed light on the offender, there are more options. **Spybot Search and Destroy** is a free and easy program that scans for all kinds of malware and removes most of it - <http://www.safer-networking.org/en/index.html> Another good choice is **a-squared**, which is free for home use. **A-squared** does a good job of detecting and removing spyware, trojans, backdoors, dialers and keyloggers. You can get it here <http://www.emsisoft.com/en/software/free/>

#### Always have a Backup Plan

Accidents happen. A bad dose of malware can scramble a PC's brains so badly that a full re-install may be the only option. At a time like that, having a recent backup of your data at hand is more than useful. Sadly, backing up PCs is a subject that rivals safeguarding nuclear reactors in complexity, so we can't plumb the depths here.

Home users can burn their documents to CDs or DVDs, but that doesn't work with email folders and other tricky stuff like Favourites, system settings for Windows and so on.

The better commercial products take care of these difficult customers. We like **Genie Backup** - <http://www.genie-soft.com/> - because it makes the job really simple. **Genie** will back up to just about any storage device you can name, or to a server on your network, either on schedule or on demand.

For synchronizing data between different systems, we use **SyncBack SE** - <http://www.2brightsparks.com/syncback/syncback-hub.html> . The program also provides a full range of backup functions but is not quite as easy for users new to the arcane science of backing up PCs.

Another option is 'disk imaging' software, which makes a copy of your entire system that you can simply roll back if things go badly wrong. It's an all-or-nothing solution and, if your last copy was made after you got infected, you'll get the malware back again. Aside from that, disk imaging is a fast and easy way to restore complete systems.

Our choice here is **Acronis True Image** - <http://www.acronis.com/>. If you have a Seagate or Maxtor disk drive, you can get an OEM version for free from the manufacturer—see [Seagate Disk Wizard](#) in the Super Software section.

We found these products the easiest options for non-technical users. Whichever program you choose, it must work reliably and provide sensible options for restoring backup data.

It's also important to keep a copy of your backups off-site in case of theft or fire. It's relatively easy to replace PCs and related hardware, but data can be as precious as the family's heirlooms and photo albums.

**[PART 1 – STAYING OUT OF TROUBLE](#)**

**[PART 2 – SCAMS AND SPAMS](#)**