



## The Technological Battle Against Malware

Mike Goyins

### Centurion Technologies

512 Rudder Road  
Fenton, Missouri 63026  
St. Louis County  
Toll Free: 800.224.7977  
Smart-Restart.com





## Traditional methods of detecting and eliminating malware do NOT work

This is becoming a depressingly true reality to nearly all computer users in today's environment - especially after you realize that despite all of your best efforts, your computer is still infected by malware. Malware is basically any program that is harmful to either your computer or to you. This harm may come in the form of spyware - programs spying on your computer and/or internet activities and then reporting that behavior to some stranger; viruses - seeking to do actual data damage by over-writing your files; or worms; trojans; etc.

Graham Ingram, general manager of the Australian Computer Emergency Response Team (AusCERT) is quoted as saying "The most popular brands of antivirus on the market... have an 80 percent miss rate [of malware]. That is not a detection rate; that is a miss rate." He goes on to state "What is happening is that the bad guys, the criminals, are testing their malicious code against the antivirus products to make sure they are undetectable." Researchers at the University of Michigan's Electrical Engineering and Computer Science Department issued a report stating, in part: "antivirus techniques failed to detect or provide labels for between 20 to 62 percent of the malware samples. Antivirus products are inconsistent at best when it comes to identifying attacks such as worms, phishing and botnets."

So, what are your options for trying to maintain a malware-free computer? Well, the first option is probably the cheapest; never hook your computer to the internet, never introduce outside programs via CD, USB, or any other source - basically, place your

computer in a "bubble" by itself. Cheapest, yes... Practical? Definitely, "no". Unless your sole use of your computer is as a very expensive deck of cards with which to play solitaire, this is not a viable option.

The second option is somewhat better, but as seen above, not by much. Traditional antivirus and anti-malware programs are purely reactive in nature. They rely on virus "definitions" and /or heuristics to identify and try to protect your computer from the malware that is known at the time. Definitions

depend on various pieces of code from known viruses and malware. All these pieces of code are stored in a central "dictionary" and then programs are compared against these code pieces to see if any matches occur. As can readily be seen, even the

smallest change to the virus or malware code would result in a match NOT being made - a "miss." The use of heuristics as a test involves basically putting the suspected program on a "watch list" to see how it behaves. Certain "bad" behavior has been pre-determined by the antivirus/anti-malware vendors. Any program doing one of these "bad" things is then flagged to the user as possible malware.

Comparing every new program to a dictionary or placing it on the "watch list" to determine its behavior, tends to be a real resource drain on your computer. In other words, this can slow your computer down to just a bare crawl. Add in the fact that you must update these definitions nearly daily AND pay a yearly subscription fee to do so, and you find that it's just not worth it.

A third option relied upon by many people is the built in "System Restore". However, this is a very hit-

**"...The bad guys, the criminals, are testing their malicious code against the antivirus products to make sure they are undetectable."**

-Graham Ingram, general manager of the Australian Computer Emergency Response Team (AusCERT)



or-miss solution. Malware writers have learned how to turn this off or cripple it to the point of non-usability. Even if there isn't any malware present on your computer, "System Restore" can fail to make its restore points for a variety of reasons: a) your "free" disk space falls below the pre-set threshold; b) "Task Scheduler" isn't running or has crashed for some reason; c) System Restore only works with the computer on and idle, if in use all the time it's on, no restore point is generated. Even if it does work, it's a simple matter for a malware program to delete the file that everything is stored in for the restore point. Once that file is deleted, that restore point no longer exists and is invalid.

The fourth option is a full system backup and restore. Show of hands – how many people have ever actually done this – and then kept up with it on an incremental, daily basis? Answer: virtually no one. Besides the time required keeping up with this option, there is the expense to consider for the backup media and equipment. With today's increasing hard drive sizes, it could potentially require several dozens – if not even a few hundred – CDs and/or DVDs to complete the entire backup of a decently loaded and used computer. Even using re-writable media, the sheer volume of disks would be astounding. I recently backed up my server to DVD. I have 750 GB of disk space with 622 GB used. It took an astonishing 144 DVD-Rs!!! Wow... Plus it took me nearly 60 hours of actual backup time... Mind you, this is the amount of time the media was actually being burned – not the total elapsed time for the backup – that took me just over two and a half weeks as sleep and work got in the way. Truly practical as an option? I think not.

The best option seen to date is a new product called Smart Restart®. Based on a "Three Zone" architecture, this seems to be the best of all scenarios. With Smart Restart protection enabled, the first of

the three zones, "Protected Zone", does just that – it basically write protects the critical portions of your hard drive and prevents malware from being able to do any permanent damage to these core operating system components. As a program tries to make modifications to files in this "Protected Zone", Smart Restart automatically redirects these changes to the second zone, the "Temporary Zone". Upon restart of your computer, all changes in the "Temporary Zone" are eliminated. The third zone is called the "Keep Zone". Basically, the users' profiles are kept here. A users' profile includes things like "My Documents", "My Pictures", "My Music", desktop folders, etc. This "Keep Zone" allows the user to save information and keep that information from boot to boot – unlike the stuff in the "Temporary Zone" that gets wiped out upon restart. When permanent changes are desired to be made to the files in the "Protected Zone", a simple entering of a password to disable protection and a restart of the computer is all that is required. Changes can then be made to the computer – under explicitly controlled conditions – and then protection can be re-enabled and you are all set - - and safe.

Smart Restart's answer to malware is to be proactive and block any malicious changes to protected files. There are no definitions to be downloaded daily and there is no yearly subscription fee. Save your documents; save your music; save your pictures of your loved ones - - all the while, saving your computer from the threat of viruses, worms, trojans, and other malware present out there.