

31 July 2006

By: Marius Oiaga, Technology News Editor



## **Suicidal Malware Rises New Threats**

*Claims Brian Denehy from CyberTrust*

Experts at CyberTrust, a security company based in Herndon, Virginia, have brought to the public's attention a new security issue related to suicidal viral threats. The latest breed of malicious software is not only equipped with stealth capabilities but is also designed in such a manner to avoid capture. As polymorphic techniques come once again in the spotlight, malware writers are also effortlessly at work to design additional protection for their creation. In this context, Brian Denehy, security assurance engineer at CyberTrust commented at the IT Security in Government Conference in Canberra on a new method implemented by attackers. He stated that viruses are designed with self delete functions triggered by the complement of indented tasks or by the necessity to avoid leaving any evidence of the cybercrime. "Some just do a complete wipe on the disk--equivalent to a low level format--to make sure that some of the remnant magnetization is not left behind. Most of you may well appreciate that just writing on a hard disk still leaves evidence there that can be recovered with the right tools. People also use the slack space at the end of files or introduce extras in the bad sectors list to hide their data ... it makes life more difficult," explained Denehy, stating that it has become increasingly difficult for forensics experts to diagnose and to emit treatment for such breeds of malware.