

# IT Backbones™

## Software News



Just Load IT - Dedicated To The Software Sector, Featuring News, Press Releases, IT Directory & Links

[Home](#)[About Us](#)[Contact](#)[News Archive](#)[Submit PR](#)[Product Reviews](#)[Web PR](#)[Briefings](#)[Advertising](#)[Pricing](#)

- [ITReseller.com](#)
- [Video News](#)
- [IT Surplus](#)
- [Events Diary](#)
- [Quick2IT](#)
- [Need2Source](#)
- [Time & Money](#)
- [Free Web Conferencing](#)

## MicroWorld Announces No Rootkits In Their Software

Published 19th January 2006

The recent controversy on the use of “rootkits” by some of the leading antivirus software vendors in their products, is gaining momentum around the world. The original rootkit controversy started with by the findings of Dan Kaminsky, an independent security researcher, on CDs produced by a leading music company. He discovered the evidence of a "rootkit" stealth for enabling copy protection on many of its CDs. Today, the global music giant faces torrential criticism and potential lawsuits on this dangerous security loophole. They are in a process of replacing the affected CDs across the globe, estimated to be half a million in numbers.

Now the findings that some antivirus companies are also using similar rootkits in their security solutions gives a completely different dimension to the issue. One of the major vendors gave an explanation that this was intended to hide the said directory from Windows APIs as a feature to stop customers from accidentally deleting files.

Rootkit is a set of software tools that are used to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge. They are known to exist for a variety of operating systems such as different versions of Microsoft Windows, Linux and Solaris. The files in such a hidden directory or location will not be scanned during scheduled or manual virus scans. This

provides a perfect hiding location for Trojans, viruses and other Malware. Needless to say, a directory that goes unscanned by the security software becomes a huge strategic risk that can become lethal for your computer.

“To MicroWorld, this is an ethical question. It’s about basic principles. We will never have a component bundled in our software that will even remotely be harmful to the user, in short run or long run. We categorically state that MicroWorld does not subscribe to rootkits or any such harmful hidden components in our software products.” said the MicroWorld spokesperson, making clear their stand on the controversy.

The antivirus software companies have larger social responsibilities. Today governments around the world and agencies like FBI and Interpol continuously seek help or work with security firms in tackling cyber crimes and organized scams. It’s imperative that antivirus providers will have to keep this big picture in their minds with every move they make. The larger implications of individual components used in the software need to be evaluated in a predictive manner to make sure that nothing harmful is shipped to the end user.

## Company Profiles powered by ITReseller.com

- MicroWorld Technologies Inc - [View profile](#)

---

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.