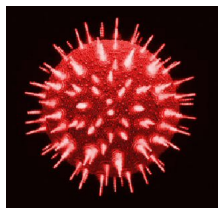


11 February 2008

By: Vlad Constandes, SEO News Editor



The way Symantec sees Virut

## [Hacked Antivirus Site Delivers Virus](#)

*Nobody's safe nowadays*

'Things just ain't the same for gangsters,' Dr Dre said in his album, 2001. He couldn't have said it better to explain the situation AvSoft Technologies' situation even if he had wanted to. It seems it's not enough to be developing antivirus software in order to protect your clients' computers and have a reputation for that, you gotta play it safe and look after your own back as well. Roger Thompson, chief research officer with security vendor AVG, told PC World that "They [AvSoft] let one of their pages get hit by an iFrame injection. [...] It shows that anyone can be a victim. ... It's hard to protect web servers properly." iFrame attacks have been very common in the past months, as they exploit a technique frequently used by web developers to insert content into their web pages. Another opinion, that of McAfee Security Research Manager, Dave Marcus, says that the site was probably compromised by taking advantage of a web programming error, most likely in the site's SQL or PHP code. Experts agree that hackers wrote automated programs that search for exactly this type of flaw and they automatically infect the respective site. The software being installed on users' computers is a variant of the Virut virus family, a 'parasitic infector' virus that is extremely difficult to remove. Ironically, AcSoft specializes in recovering data lost due to virus attacks. If you got infected by going to the company's download page, chances are you'll be hitting it again, to download their tool for mending the situation. Vicious circle? The upside, if the term doesn't seem ironic, is that the version automatically installed on page access is not a very complicated one, that only hones on the well-known bugs, so if the system is patched as well as possible, the loss won't be all that great. AvSoft wasn't available for comment, but if you're using their software, you'd better clear off of their download page until something certain is posted on the company's site.