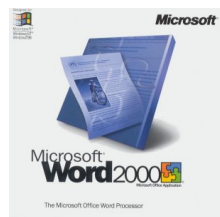


12 October 2007

By: Alexandru Dumitru, Security News Editor



## [Word Crashes, Viruses Land](#)

### *Symantec tests Microsoft vulnerability*

I guess some of you are sick of just reading "do this, patch that to stay secure" with explanations written in such a techie language that you do not understand a thing. Well, I'm now going to explain nice and simple why it's important to patch Microsoft products. If you've read the recent news or have been simply paying attention to what your computer is prompting you (if you have Windows on it, that is), then you know that Microsoft has issued several patches in order to fix security vulnerabilities in their software. Security experts recommend patching up quickly, but no one has actually given any simple examples of what could happen, until now. Symantec has analyzed a file sample that has been shared with them, to better explain what was actually wrong with Microsoft Word. It was a classic .doc file and when they opened it, the file would cause the program to crash. It made any version go down, except the 2007 one. In their analysis, they found out that the document contained shell code and three other pieces of malware. However, this was no regular Word document, like the one I'm writing this piece of news in. It wasn't in OLE format, and after further investigation, they disclosed that it had been created in Word for Macintosh. That document exploited a vulnerability in Word (for Mac) that Microsoft recently patched. So there you have it, unless you patch up, you can have some serious issues. This file is detected by Symantec's anti-virus product as Trojan.Mdropper.Z and it will install a dropper, a backdoor and a rootkit. You can see the full analysis [here](#). I think I've made things pretty clear in this article, so that you understand how important plugging security holes is!