

23 February 2006

By: Victor Mihailescu, Apple News Editor



Sophos Anti-Virus Software Causes More Damage Than All OS X Viruses, Trojans and Worms Put Together

Who will protect Mac users from the anti-virus companies?

After trumpeting the Inqtana-A virus just days ago and making a big deal out of this worm that relies on a security flaw patched by Apple over half a year ago, anti-virus vendor Sophos has now taken another bold step towards the grave. Their update for the Inqtana-B virus identity file incorrectly flagged various Microsoft Office and Adobe Acrobat Reader files, to name just a few, which led to data loss for many of the program's users. Hundreds and in many cases thousands of files were erroneously flagged as being infected, and, depending on the settings of the users, were then deleted. In several cases the spread of the 'infected files' was so great that after the 'disinfection' the systems were left all but useless. The Mac community is in an uproar after this incident, which only served to bring up memories of the problems encountered with Norton's Anti-Virus Software. The fact that the Inqtana-B problem the update was supposed to address was so remote only puts the integrity and moral practices of Mac anti-virus program vendors under scrutiny. The two 'viruses' and the 'extremely critical' OS X flaw all combined did not even cause a fraction of the damage the Sophos software did. The Leap-A worm infected less than a hundred machines, and of those, all had been willing infections on behalf of testers and researchers; the Inqtana-A worm had spread even less seeing how Apple had closed the hole it needed more than half a year ago. After the entire media was in an uproar about how threatened OS X now is because of the high public profile, the most damage is still coming from companies and programs who are supposed to be preventing the damage in the first place. At the end of the day, the only questions that begs to be asked is: Did the people at Sophos even test their software? At least once? How could this happen? Who will protect Mac users from the anti-virus companies?