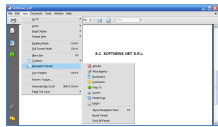


6 May 2008

By: Traian Teglet, Technology News Editor



Adobe Reader in action

## [Adobe Acrobat Reader and Professional Vulnerability Reported](#) *Update recommended*

It seems that Adobe Acrobat Reader and Professional users have been and probably still are vulnerable to dangerous attacks. The vulnerability has been discovered by one of the largest security company, Symantec. According to Symantec's webpage, the security issue is part of the Neosploit exploit toolkit and has been created to take advantage of a February 2008 vulnerability in the above mentioned Adobe applications. Almost any browser you may use is vulnerable to this attack vector, which has been designed to work relatively silently. A user only needs to browse the Internet using whatever browser is available on a computer with Adobe's Acrobat previously installed. After these conditions are carried out, the user is lured to unprotected websites leaving his computer infected. The way this exploit works is largely familiar, as an increased number of websites bring pop-up windows that you end up clicking without choice. What you need to do in order to ensure that you aren't affected by this exploit is to upgrade to the latest Adobe Acrobat and Reader. The 8.1.2 version is said to be secure and everything prior to this release will most likely render you vulnerable to attacks. Being the company that has discovered the vulnerability, Symantec has worked alongside Adobe's Security team in order to make this last patch safe. Any user of Symantec's IPS-enabled client will be protected, as the application will prevent this PDF attack and will recognize it as HTTP Malicious Toolkit Download Activity or Trojan.Pidief.C, depending on the used client. Adobe's products usually have an upgrade session, but it is wiser to manually install the new patch as soon as possible. Doing so will make your computer safe from any potential attack, which will unlikely be noticeable. You can download the program, right here at Sofpedia using this [link](#).