

## PDF files may contain malicious code

**P**ause...before you open that pdf attachment, because now, even pdf or portable document format files can contain malicious code.

IT security firm F-Secure last week issued a warning that it has recently seen tens of thousands of such malicious pdf files being spammed via mass e-mail messages.

When such pdf files are viewed on vulnerable machines, those PCs get infected.

According to F-Secure, the malicious file exploits a recently discovered frailty in Adobe Acrobat and Internet Explorer 7 and downloads more vicious programs (malware) from a server in Malaysia.

The aim seems to be to create a network of infected machines to be used as zombie machines to snare other PCs.

The evil e-mail contains subject lines like "Your credit report" and "Personal financial statement" and has no content in the main body except for the report.pdf attachment. F-Secure's chief research officer Mikko Hypponen said: "We are worried

about this case, as pdf attachments are typically not filtered at e-mail gateways.

"Executable files are now stripped almost everywhere, but pdf is stripped almost nowhere."

This vulnerability was made public by a researcher called Petko D. Petko in September in his blog. Adobe acknowledged the chink in the armour as a critical vulnerability via a security bulletin released last month.

This issue affects only users running Adobe Reader or Acrobat versions 8.1 or earlier on a Windows XP or Windows 2003 machine with Internet Explorer 7 installed. Adobe added that the problem can be fixed if users update to Adobe Reader 8.1.1 or Acrobat 8.1.1.

Another IT security firm Fortinet said it saw high activity with this exploit on Oct 27, but added it has recently subsided.

"Since this is a new exploit, there will certainly be more activity on this front, and it is something users should be aware of," said researcher Derek Manky from Fortinet's Global Threat Research Team.