TechTarget
Security Media

SearchSecurity.com SearchSecurity.co.UK SearchSecurity.in SearchFinancialSecurity.com SearchMidmarketSecurity.com
SearchSecurityChannel.com INFORMATION SECURITY DECISIONS FINANCIAL INFORMATION SECURITY DECISIONS INFORMATION SECURITY

SearchSecurity.com E-Guide

How to Secure a PDF File

Sending sensitive information in a pdf could be unsafe, and depending on your organization's security policies, could land you in a lot of trouble. In this expert Q&A, Michael Cobb explains how to avoid malicious content that is embedded into .pdf documents.

TechTarget
Where Serious Technology Buyers Decide

ESET NOD32 Antivirus 4

Fast, Effective, Proactive, Antivirus and Antispyware

Our award-winning proactive threat-detection technology delivers the most effective protection from viruses, spyware, and other internet threats. ESET software blocks most threats the moment they are released, avoiding detection latency common to competing products. And with super-fast, super-easy operation, we keep your users productive, and your help-desk load down.

www.eset.com

eset

How to Secure a PDF File

by Michael Cobb, featured expert

Question:
What are ways to make sure that malicious content isn't embedded into documents and .pdfs?

Answer

There are two possible ways to interpret your question. One: How do you ensure that documents you receive or use don't contain malicious content? And two: How do you prevent malicious content being added to your own documents? I'll cover both issues to ensure I answer your question.

The way to tackle the first problem of avoiding malicious content embedded into documents is to ensure that:

1. Your operating systems and all applications are kept up to date with the latest patches.

2. Antivirus, antispyware and firewall applications are installed, up to date, and running.

3. Documents are always scanned before being opened and users never open documents or links received unexpectedly or from unknown sources.

4. Some form of antiphishing service is installed on the network.

The first three recommendations are pretty much standard security practice. Many attacks use newly discovered vulnerabilities, like the recent Adobe Flash player vulnerability, to embed and execute malware within a document. Therefore, keeping systems patched and keeping malware tools up to date with the latest signatures will greatly reduce the chances of such attacks being able to successfully infect your machine. Documents should always be scanned before being opened, and the settings on applications such as Word and Excel should prevent any macros embedded in a document from running without your explicit consent.

Your fourth layer of defense is not so widely used, but is becoming essential. Zero-day attacks can be lethal until vendors and AV products release patches or signature updates for their products. In order for hackers to launch such attacks, they need to entice victims to visit a particular website, which they try to do using phishing techniques, such as sending emails with enticing offers that link to their malicious site. An antiphishing service, such as that provided free by OpenDNS, blocks access to sites that are suspected of being malicious. This protection also helps safeguard those users who still insist on clicking on links from unknown or untrusted sources.

Problem two, how to secure a .pdf file or document from being infected with malware, requires a data and document lifecycle management system to protect documents at rest, in transit and when being accessed, shared or published. Besides encrypting and enforcing strict access controls, you should also aim where possible to have security reside within a document, to protect it as it moves through its lifecycle inside and outside the organization. Probably the most common way of achieving this protection is by using Adobe PDF files. PDFs include built-in controls to limit who can open and print them and how long recipients can access them. The files can also contain tracking to show who received them and if the files were opened.

Even if you use a rights management scheme, you are possibly open to other malware attack vectors if you share documents via a website that runs third-party ads or allows user input. Hackers can use cross-site scripting attacks to inject malicious code directly into your webpages if the site doesn't thoroughly validate user-generated input, received, for example, via a comments form.

Hackers are also using ads displayed on genuine sites as a way to inject malicious content or direct users to a malicious website. The Google Adwords service, for example, has been used to serve text ads that infect vulnerable Web surfers by routing them through an intermediate, malicious site. If you don't need to serve ads or show other third-party content on your site, then don't; you can immediately remove this attack vector.

Michael Cobb, featured expert, *Founder and Managing Director, Cobweb Applications Ltd.*

Michael Cobb*, CISSP-ISSAP is a renowned security author with more than 10 years of experience in the IT industry and another 16 years of experience in finance. He is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. Michael is also a Microsoft Certified Database Administrator and a Microsoft Certified Professional.*

Resources from ESET

Conficker by the numbers

Ten Ways to Dodge CyberBullets

ESET NOD32 Antivirus 4

About ESET
ESET provides award winning security solutions that combined fast system scans with the ultimate in proactive protection against both known and unknown online threats. ESET NOD32 Antivirus was awarded "The Best Proactive On-demand Detection" and "The Best Overall Speed Performance" for 2008 by AV Comparatives.

By delivering state-of-the-art endpoint security, ESET Smart Solutions™ increase your security while reducing your TCO. ESET's updated Remote Administrator, delivers a highly scalable enterprise-ready defense against malware, reducing your attack surface resulting in fewer help-desk loads. A light system footprint and blazing fast scanning speed can even extend the useful life of PCs and laptops.

ESET has also been named to the INC500 for the third consecutive year, and has an extensive partner and customer network, including corporations like Intel, Canon, Dell and Microsoft.