

Stay Smart Online Alert Service Newsletter

March 2009

Overview

The purpose of the Newsletter is to provide general advice about online security issues and help you learn to better manage the security of your computer and information when online.

The Newsletter provides additional information about the threats and software bugs which were reported during the period, or about other threats to be aware of.

Feedback

Thank you to those subscribers who have provided feedback to our Alerts, Advisories and Newsletters. We are very interested in your feedback and where possible take on board your suggestions or requests. In this newsletter we have responded again to feedback questions.

Common online threats

Sometimes criminals use telephone services to trick you into taking action which can harm your computer

Recently there have been some Australians who have received text messages on their mobile telephones which claim that their online banking details have been stolen or compromised. The text message includes a web link which provides further information. If you then use a computer with Microsoft Windows installed to visit the web site with your web browser, it will in all likelihood install malicious software (malware) on your computer. At the time the message was circulating, only a few anti-virus programs detected the malware.

This is just a reminder that sometimes criminals use mobile telephones, in addition to email and web sites, as a way to get your attention and trick you into doing something which could harm the security of your computer and your personal information. This is referred to as an “out of band” attack, and tricks like this have the capacity to allow a criminal to take control over your computer without your knowledge.

SMS (for Short Messaging Service) is a written or text based communication that is sent via mobile telephones. SMS is also referred to as text messaging or “texting”.

Feedback questions

This section is devoted to responding to feedback or questions submitted by people who have subscribed to the Stay Smart Online Alert Service.

Can the government provide free anti-virus and anti-phishing software for pensioners and low-income earners?

There are already a number of effective products available which provide the functionality you require free of charge.

We recommend a number of anti-virus products that are free for non-commercial use which are suitable for pensioners and others on low incomes. Many in the information security community use these products on their own home computers and recommend them to friends and family. Therefore if you are constrained by a budget, these products are highly recommended.

If you have a commercial anti-virus product on your computer that has expired you will not be able to obtain signature updates for it. Unless you are prepared to pay to renew your subscription, you should uninstall the product and install one of the free products. Do not attempt to install a second anti-virus product without first uninstalling the previous product.

The key point is to have an anti-virus product AND an anti-spyware product installed whether it is a free or a commercial product and then *to keep them up to date* at all times.

The following are some free security programs. However, some of these are only free for non-commercial use. This means they are suitable for ordinary home internet users but not for businesses. You should always read the licensing conditions for the individual product you are about to install.

Anti-virus software

[Antivir](#)

[AVG](#)

[Avast!](#)

Anti-spyware software

[MacScan](#) (for Apple Mac OS X only)

[Windows Defender](#) (for Microsoft Windows only)

Spam filtering software

[Mail Washer](#)

[SpamPal](#)

To help you identify and prevent phishing attacks we recommend activating the built in phishing-detection features in current versions of the Microsoft Internet Explorer web browser or the Mozilla Firefox web browser (both of which are free). See the SSO Factsheet, [how to detect phishing sites and steps to prevent being fooled by them](#), to find and activate these features.

Zombie Awareness Week

Last week, the Australian government and the Internet Industry Association conducted a number of events designed to raise [public awareness](#) about “zombies”. For some readers the term “zombie” might be new and imply this is a new problem. This is not the case – this is a problem that has been around for a number of years but sometimes new labels are given to explain things which become commonplace.

Unfortunately, the problem of compromised computers (or zombies) is a serious one, and around the world at any given time there are millions of compromised computers being used for criminal purposes.

What is a zombie?

The term “zombie” is a term to describe a computer that has been successfully attacked by a criminal and which is now under the control of a criminal for criminal purposes. Other terms which mean the same thing are “robots”, or more commonly “bots” for short. These terms are used because your computer effectively becomes a remote-controlled “robot” (for use by a third party) that comes alive without your control like, you guessed it, a “zombie”.

The term “botnet” refers to a group of bots or zombies which is under the control of a criminal. The number of compromised computers in a botnet is generally in the hundreds and often many thousands.

Computer zombies or bots may appear to work and operate normally, but a person in a remote location has, through a variety of potential methods, managed to open a secret “backdoor” to that computer. Via the Internet, that person is able to conduct a variety of criminal activities using the compromised computer, mostly without the user’s knowledge.

Such computers are also said to be “compromised” – that is, the security of the computer is compromised and the confidentiality and privacy of the information on the computer no longer remains solely with the owner or legitimate users of the computer; also the criminal has the ability to delete or modify information or system files on the computer, which may mean you lose important documents or reports or it may cause your computer programs to not work properly or slow down.

How are zombies created?

Compromised computers or zombies are those which have been successfully attacked by criminals. Criminals do this in a variety of ways. The most common methods are:

- by exploiting a known software bug. This is why it is important to check information about software bugs sent by the Stay Smart Online Alert Service or on the Stay Smart Online Alert Service web site. If you have any of the affected software programs on your computer, take the necessary action to update the software to fix the bug or problem.
- by fooling a computer user to install malicious software (malware) on to their computer. The malicious software may be an email attachment or a link in an email to a web site. Sometimes criminals compromise well-known popular web sites and install malware on the

web site that is not readily visible to ordinary users but will automatically install on the user's computer as soon as the user's computer connects to (or opens) the web page.

- by sharing infected USB drives (also called memory sticks or thumb drives) between computers.

How can I stop my computer from becoming compromised?

The Stay Smart Online Alert Service exists to help give ordinary people useful information, in simple language, to prevent your computer from being successfully attacked by criminals and compromised.

There is no doubt that the online environment has brought significant benefits and advantages to many people in the community, but there are some risks which are, for many people, unseen and hidden. It is important for users online to understand these risks and take appropriate precautions. While risks can never be completely eliminated in any aspect of life, they can be significantly reduced online by applying commonsense, keeping up to date and acting on the advice provided here as part of the Stay Smart Online Alert Service.

Software bugs

Security bugs in the software installed on your computer make a hole in your computer's security defences. This hole makes it much easier for criminals to attack your computer and steal useful information from it, or take control over your computer without your knowledge. This is why it is important to apply software updates provided by vendors as soon as possible. Installing software security updates as soon as they are available closes the security hole and reduces the risk to your computer and your personal information and files.

Occasionally information about a new security bug is released to the public but the vendor does not yet have a software update ready. This situation occurred again recently with Adobe Acrobat and Adobe Reader. Adobe Reader is available for download free of charge and allows you to read PDF files. It is recognised by the following logo. Adobe Acrobat has similar functionality but is not free.



In February, we issued an [SSO Alert AL2009-007](#) about this problem which also provided information about the steps you can take to protect yourselves in this situation. However, Adobe has since released software updates to fix this problem, so you can now apply the software updates outlined in [SSO Alert AL2009-010](#).

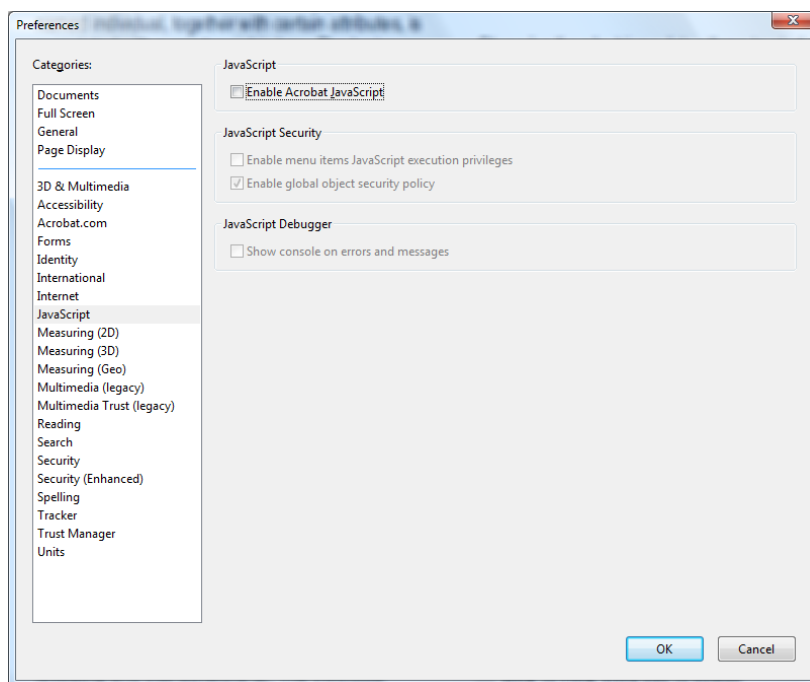
A criminal could exploit these bugs by convincing a person who has Adobe Reader or Adobe Acrobat installed on their computer to open a specially crafted PDF file, either as an email attachment or by clicking on a web link. Alternatively, a person may become infected by simply visiting a web site that has been compromised by a criminal who installed a harmful PDF file. Criminals are known to be exploiting these bugs and so the need to update the software is highly recommended.

What you can do

If you have either Adobe Reader or Adobe Acrobat installed on your computer apply the software updates outlined in [SSO Alert AL2009-010](#).

In addition it is recommended to de-activate one of the functions in Adobe Reader and Adobe Acrobat, which would allow a criminal to exploit this security bug. Turning off this function, which is called JavaScript, makes it harder for the criminal to exploit this particular bug.

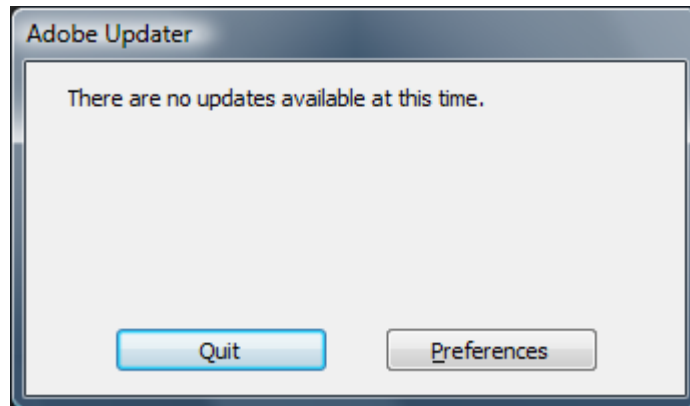
To do so, open Adobe Reader and/or Adobe Acrobat. Select the “Edit” menu, then select “Preferences ...”; select “JavaScript”, which will then display a window as follows.



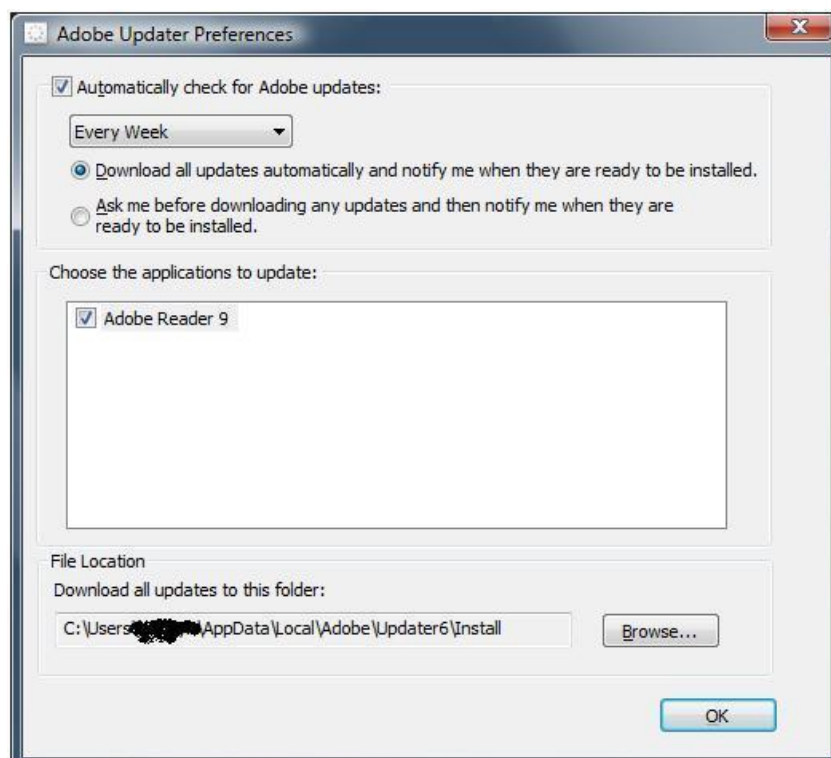
The “Enable Acrobat JavaScript” is ticked by default. Make sure “Enable Acrobat JavaScript” is not ticked as shown above. Click OK and close.

Setting up automatic updates in Adobe Reader

To set up automatic updates in Adobe Reader, open Adobe Reader and select the “Help” menu, then select “Check for Updates ...”. This process will also manually check for updates. It will then show the following pop-up window, with a message that indicates if your version of Adobe Reader is already up to date or not:



Select “Preferences” to set up automatic updates.



Check the settings are the same as above. Then click OK.

Disclaimer

This Newsletter has been prepared by AusCERT for the Department of Broadband, Communications and the Digital Economy.

The information is intended for use by home users and small to medium sized businesses and is general information only and not intended as advice and was accurate and up to date at the time of publishing. The material and information in this newsletter is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. In any important matter, you should seek professional advice relevant to your own circumstances.

The Commonwealth, AusCERT, and all other persons associated with this Newsletter accept no responsibility or liability for information either included or referred to in the Newsletter. No responsibility or liability is accepted for any damage, loss or expense incurred as a result of the information contained in the Newsletter, whether by way of negligence or otherwise.

The listing of a person or organisation in any part of this site or Newsletter does not imply any form of endorsement by the Commonwealth of the products or services provided by that person or organisation. Similarly, links to other web sites have been inserted for your convenience and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

Please note that material in this Newsletter, as the case may be, includes views or recommendations of third parties, which do not necessarily reflect the views of the Commonwealth, or indicate its commitment to particular course of action. Material on this site or in this Newsletter may also include information provided by third parties. The Commonwealth cannot verify the accuracy of information that has been provided by third parties.