

**Subject:** \*\*\*Conficker: Information Security Alert, 03/31/09\*\*\*  
**From:** Office of Information Technology <OIT@utsa.edu>  
**Date:** Tue, 31 Mar 2009 12:45:15 -0500  
**To:** "EVERYONE (The entire UTSA organization)" <EVERYONEALL@utsa.edu>

The UTSA Information Security Office has been monitoring the status of Conficker, a high-profile security threat. Security experts are expecting Conficker to become active on Wednesday, April 1, 2009.

What is Conficker?

The Conficker worm is a type of malicious software (malware) that first appeared in October 2008 and targets the Microsoft Windows operating system. A great number of unpatched personal computers around the world have already been infected by Conficker.

What will Conficker do?

Information Security experts are unclear on what will happen to the infected computers on April 1. The activation could cause the virus to take any of several actions from attempting to steal sensitive and/or confidential information to attempting to cause computer outages to simply waiting for additional updates. The overall effect of the virus update could be disruptive or appear to be benign.

Is your PC infected?

One of the symptoms of a Conficker infection is that it does not allow your PC to retrieve updates. To check if your PC has been infected by Conficker, open a browser (Internet Explorer, Firefox, etc.) and navigate to one of these Web sites:

<http://www.mcafee.com>

[http://www.symantec.com/norton/theme.jsp?themeid=conficker\\_worm](http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm)

<[http://www.symantec.com/norton/theme.jsp?themeid=conficker\\_worm&inid=us\\_ghp\\_link\\_conficker\\_worm](http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_ghp_link_conficker_worm)> &inid=us\_ghp\_link\_conficker\_worm

<http://www.microsoft.com/protect/computer/viruses/worms/conficker.msp>

If your computer is infected with Conficker, you will not be able to display any of these Web pages. Instead you will see an error. If you believe your computer is already infected, shut down your PC and contact your department's computer support personnel or call the OIT Help Desk at 458-5538. More information on Conficker is available at

[http://www.utsa.edu/oit/security/sec\\_Conficker.html](http://www.utsa.edu/oit/security/sec_Conficker.html).

Are Macintosh PCs affected by Conficker?

No. Conficker specifically targets Windows-based machines. However, there is malware that targets Macs, so please be sure that your Mac is set up to receive automatic updates.

How can I protect against Conficker?

Before you leave work today (3/31), shut down your PC completely. When you

turn on your PC tomorrow, any pending updates will be applied. All computers that are managed by the UTSA Office of Information Technology have been updated with the most recent antivirus and operating system patches. If you use a UTSA-owned laptop at home, please be sure that it is set up to receive automatic updates.

#### Security Tips

The Information Security Office suggests that you always exercise caution when opening e-mail messages and when you access the Internet.

- Avoid visiting untrusted Web sites
- Do not open unsolicited e-mail messages (e-cards, invitations etc.)
- Do not click on any links in unsolicited e-mail messages
- Do not open suspicious e-mail attachments
- Ensure that your PC is set up to receive automatic operating system updates
- Use anti-virus software

#### More Information on Conficker

Please visit the OIT Web site Conficker FAQ for additional technical information: [http://www.utsa.edu/oit/security/sec\\_Conficker.html](http://www.utsa.edu/oit/security/sec_Conficker.html)

The Office of Information Technology