

**Computer Troubleshooters
Toowoomba East**
15 Diagonal St
Toowoomba

office@ctstoowoomba.com.au
www.ctstoowoomba.com.au

**T: 07 4636 6025
F: 07 4636 6276**

Offices Worldwide

Australia, Austria, Bahrain,
Botswana, Bulgaria, Canada,
Colombia, Egypt, Ghana,
Greece, Guatemala, Hong Kong,
Ivory Coast, Kenya, Kuwait,
Malaysia, Netherlands, New
Zealand, Nigeria, Philippines,
Republic of Ireland, Saudi Arabia,
Singapore, South Africa, Turkey,
United Kingdom, United States of
America

International Website

www.comptroub.com

Computer Troubleshooters
The World's #1 computer service
franchise network

OVER
450
LOCATIONS WORLDWIDE



Global Newsletter May 2011



Watch out, bots – here comes the FBI!

The Federal Bureau of Investigation wants access to computers in the United States, but this might be a good thing. In an unprecedented move, the FBI has gained access to the 'command and control' servers that have been controlling the internet nasty 'Coreflood'. With this control, the FBI could use these servers to send a command to all infected computers to uninstall the Coreflood software.

Coreflood has actually been around since 2002. Known as a 'botnet' it works by infecting your computer through a file that you open or a link that you click on, which is disguised as something you might want to read. In the background, the software embeds itself into your computer and starts communicating back to the control server, doing whatever it is told to. These commands could range from the annoying (changing your wallpaper, opening your CD tray, randomly playing sounds or shutting down your PC) through to the dangerous (recording your keyboard strokes & sending your personal information back to the command servers).

With an estimated 2.3 million infected computers, a command to uninstall itself would be a very effective way of eradicating Coreflood. However, the FBI has to watch its step and is working with the US Department of Justice to ensure it doesn't violate the USA's privacy protection laws. It is currently seeking 'request and authorization to delete' from government agencies and corporations and may issue 'notice of infected computer' alerts through internet providers to home users.

In the meantime, Microsoft has added a further update to its Malicious Software Removal Tool to tackle the latest instances of Coreflood and this will be released to Windows computers with Microsoft's next batch of security updates. Most anti-virus software manufacturers will now also detect Coreflood on an infected computer.

While it's interesting to see the FBI taking this approach to clean millions of computers, it once again highlights the need for computer owners to be vigilant about security measures. It's easy to forget about older, rarely used computers and if their software isn't kept up to date, they can easily be targeted by botnet infections. Your security strategy needs to include regular updates to your operating system software and your security software, as well as checking that your security software is functioning correctly and performing regular scans. You also need to practice safe internet habits, such as being careful about suspicious-looking file attachments and not visiting dubious websites.

Coreflood is one of thousands of examples of botnet software currently in existence. Talk to your local Computer Troubleshooter about the best protection strategy for your computers or about any of your technology needs.



**Contact your local Computer
Troubleshooters**

**Neil Sciffer
0421 476 492**