

Has Your Browser Been Hijacked?

by Gary A. Campbell, gacWebSolutions

Being online makes your computer vulnerable to a host annoying problems: virus infections, unwanted banner ads, pop-up windows and spyware to name a just few. Here's one you may not be familiar with: it's called browser hijacking.

The symptoms are readily apparent. You navigate your way to a perfectly innocent looking site and suddenly WHAM! You're redirected to a porn site or some unheard of search engine. You try to use your 'Back' key only to find it's been disabled. Then WHAM - WHAM -- WHAM! Three more pages pop up filling your screen with useless sites. You decide the smart thing to do will be to close down and reopen your browser. But when it reopens you find it's a bit slower and your default home page has changed to some unheard of website. You've lost control of your browser. Congratulations. Your browser has been hijacked.

That perfectly innocent looking site you visited quietly downloaded a malicious executable file onto your system. This executable is responsible for your browser's odd behavior.

Not only can you be hijacked by visiting a 'carrier' site, but instant messaging programs are also being used to hijack browsers. You may think you're viewing an actual web URL or the file of a 'friend', when in reality clicking on the link or downloading the file is inviting a hijacking!

Most hijackers leave numerous executable files on your system so they will re-execute the hijack on every reboot. Some of them won't execute right away, but will after a reboot. Often each infection is worse than the last, adding different files, executables, and other garbage clogging up your system, including the registry, rendering most remedies ineffective. A very real concern is whether any of these hijacking executables contain even more malicious viruses.

The recent increase in hijackings suggests to me that the new anti-spamming laws are having an effect. I suppose that the hijackers reason that if they can't spam via email, they'll spam via browser hijacking.

A number of programs are available to detect and eliminate the malicious files on your system. In my opinion, the most reliable and thorough is HijackThis. One caveat: because of the nature of hijacking files, the remedy will involve making changes to your system's registry. And any time you mess with your system's registry you are flirting with danger. Take your time, read the help files and proceed cautiously. If you're not 100% confident (OK, maybe 90% confident) have a pro do the repair. You'll be saving yourself a lot of aggravation.

One last bit of advice: many malicious files will creep into your system restore points. For this reason, as soon as your machine is disinfected, create a new system restore point.