SearchSecurity.com
Security School

Spyware removal checklist

By Michael Cobb

Trying to remove spyware can be a fruitless and frustrating experience. The following checklist should enable you to clean an infected system, but it isn't a two-minute task. Check that you understand how to complete each step, download all the necessary programs and allow yourself plenty of time to complete the entire procedure.

1. Backup the system on to separate storage media.

2. Start the infected PC and boot into **Safe Mode with Networking**, as some spyware can only be removed in Safe Mode.

3. Turn off System Restore on Windows XP/ME systems.

4. Open Add/Remove programs and remove any application that you do not recognize and/or deem to be spyware.

5. Install a licensed antivirus product. Update and run it on the infected system.

6. Install Spybot–Search & Destroy (freeware available at safer-networking.org/en/). Update and run it on the infected system.

7. Install one, if not two, antispyware products such as Spy Sweeper from Webroot Software, Microsoft Anti-Spyware, eTrust PestPatrol or Ad-Aware from Lavasoft. Update and run them on the infected system.

8. Download HijackThis (freeware used to detect browser hijakers that's available at hijackthis.de/), start it and click the "Do a system scan and save a logfile" button.

9. Analyze your HijackThis log at the HijackThis Web site above.

10. Use HijackThis to remove anything in the “Nasty” category.

11. Reboot and run Spybot-S&D and the antispyware products you've installed until the system is clean. You may have to run them more than one.

12. Launch Internet Explorer and browse the Web to verify your Internet connection was not broken while removing any spyware. If you cannot browse the Web, run LSPfix (a free utility from cexx.org) to repair Winsock 2 settings. Perform another test.

13. Turn on System Restore.

14. Backup the system and destroy the previous backup, as this will be infected with spyware.

15. Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize the risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid e-mail scams and deal with deceptive spam.

16. A new tool that can be used to remove spyware is Microsoft's Windows Malicious Software Removal Tool, which checks computers running Windows XP, Windows 2000 and Windows Server 2003 for infections by specific, prevalent malicious software — including Blaster, Sasser and Mydoom — and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month.