The TechRepublic Comprehensive Spyware Removal Checklist

Version 1.0
May 20, 2008

By Erik Eckel

For many users, spyware has become an even bigger problem than viruses. Regardless of size, everyone from small businesses to enterprise organizations must battle the associated risks that include key trackers, Web page redirectors, persistent pop-up advertisements, inoperable network connections, unwanted tracking applications and other nefarious programs that slow and even render systems and programs non-operational.

Infected systems have become the bane of many systems administrators, consultants and support professionals. While the best spyware defense is a combination of behavior modification -- teaching users not to indiscriminately click on attachments, surf My Space and similar sites freely and engage in other risky computing behavior -- and effective, business-class protection, IT professionals are often tasked with cleaning spyware infected systems.

Methods and recommendations differ, just as with many other technology issues. When particularly problematic infections exist, some technology professionals advocate simply backing up user data, reformatting the drive and reinstalling Windows. Others believe most forms of spyware, and the related problems these infections leave behind, can be eliminated.

When systems can be salvaged, much time and expense is saved. For example, cleaning a system of spyware infections and repairing post-incident damage can save the time required to track down CDs and DVDs for previously installed programs and associated license keys (if they can even be found), not too mention the time required to actually reinstall Windows, reinstall the applications and mirror the user's previous Windows settings and application configurations.

While not every infected system can be saved, following the steps in this TechRepublic checklist can go a long way toward eliminating common infections and repairing the collateral damage.

The checklist consists of four sections:

I. Scan The Infected Drive Using A Second System

II. Perform Cleanup Tasks

III. Repair Collateral Damage

IV. Final Steps

I. Scan the infected drive using a second system

Configure a standalone test/repair system. The machine need not be a behemoth workhorse. Instead, what's most important is to create a test system that doesn't possess important data and that is separated from other computers via a hardware-based firewall.

Consider the following configuration for the test system:

- Windows XP Service Pack 2 or Windows Vista Service Pack 1.
- An Intel Pentium 4 3.0GHz or faster (or AMD equivalent) CPU.
- 1GB RAM for Windows XP; 2GB for Windows Vista.
- Windows Defender, possessing the most current updates.
- Two business-class (not free consumer-grade) antispyware applications possessing valid licenses and the most current updates.
- A business-class (not a free consumer version) antivirus application possessing a valid license and the most current updates.
- An anti-rootkit application possessing a valid license and the most current updates.

Once the test system is available:

- ☑ Remove the hard disk from the infected system (**always be sure to have a verified backup of critical drive data before testing/removing spyware**).
- ☑ Connect the hard disk to the test workstation. Several methods are available:
  - Configure the infected disk as a slave and connect it to the test workstation motherboard via an internal IDE or SATA cable.
  - Leverage a USB/IDE-PATA-SATA 2.5"/3.5" hard disk adapter.
  - Connect the infected hard disk via a USB hard disk enclosure.
  - Utilize a removable hard disk bay.
- ☑ From the test workstation, open the antispyware programs individually and run full system scans. Remove any and all infections that are found.

NOTES

- *It's important that the test system possess effective, business-class antivirus and antirootkit software. Many spyware-infected hard disks also possess active viruses and rootkits that could infect the test system upon the two drives being physically connected together.*
- *Leveraging a second system to perform the adware and spyware scans helps the antispyware applications better identify and remove dormant spyware applications from infected hard disks that aren't actively running Windows. Spyware and other malicious programs have become much more adept at hiding themselves from Windows, but when a second Windows installation is used to scan the infected drive, identification and removal rates improve.*
- *For better sanitation of an infected disk, also run complete antivirus and antirootkit scans while the drive is connected to the test workstation; remove all infections that are found.*

II. Perform cleanup tasks

Once the test workstation has completed its antimalware passes and has removed all found incidents, re-install the hard disk in the original system. With the infected system's Ethernet cable disconnected (and any wireless connection disabled), power the system in Safe Mode, then:

- ☑ Delete files from the following locations:
    - All users' temp directories
    - All users' Internet cookies and temporary Internet directories
    - The system root's temp directory
- ☑ Scour the Windows\prefetch directory for suspicious entries, deleting (or changing the name for) those that appear problematic. Before clearing the prefetch directory, review Ed Bott's thoughts on the subject.
- ☑ Empty the Recycle Bin.

Next, reboot the system, booting normally into Windows. Then:

- ☑ Disable System Restore (right-click My Computer, select the System Restore tab, check Turn Off System Restore On All Drives and click OK).
- ☑ Open the Microsoft System Configuration window (Start | Run | MSCONFIG).
    - Click the Service tab. Check Hide All Microsoft Services to reduce clutter, and disable any and all suspicious services. Click Apply.
    - Click the Startup tab. Uncheck any and all suspicious services. Click Apply.
    - Then click OK. Confirm you wish to restart the system.
- ☑ Open Control Panel's Add/Remove Programs (Windows XP) applet (or Vista's Uninstall A Program console) and remove all recognized spyware programs.
    - Pay particular attention to removing weather tools, suspicious Web search tools, BearShare, LimeWire, Kazaa, Morphus and similar applications.
    - Uninstall any free or unknown antispyware, antivirus and registry cleaning applications.

NOTES

- *When deleting temporary and other files, if specific spyware or malware files refuse to be deleted or prove to be locked, reconnect the infected hard disk to the test machine to delete these offending files.*
- *In place of Microsoft's System Configuration utility, consider downloading and installing TrendMicro's free Hijack This program, which in many cases catches many more rogue processes, browser objects and other unwanted detritus.*

III. Repair collateral damage

Many forms of spyware attack Windows' TCP/IP stack and network communications. Numerous free utilities are available for repairing Winsock, Windows Updates and other network and communications subsystems.

Based on the nature of any lingering or remaining issues or failures, consider downloading and running all of the following utilities:

- CCleaner -- Legitimate free registry cleaning application. Assists in deleting temporary files and cookies and cleaning system registries.
- Dial-A-Fix -- A simple program that often makes quick work of resetting Windows Updates, repairing SSL, HTTPS and cryptographic services and fixing COM/ActiveX object errors and missing registry entries.
- EZPCFix -- For Windows 2000/XP, helps clean a variety of malware infections.
- SmitREm -- Time-saving tool for removing common malware infections -- including AntiVirusGold, SpySheriff, VirusBurst and Winhound -- that themselves claim to offer antimalware protection.
- Spybot S&D -- The ubiquitous, tried-and-true malware detector and remover. Does not identify or remove all forms of malware, but it's a solid basic tool that includes a process explorer.
- Trend Micro CWShredder -- Defeats CoolWebSearch.
- WinSock XP Fix -- Repairs Windows XP's winsock settings and configuration.
- VundoFix -- Removes irritating Vundo (or Virtumonde/Virtumondo) Trojan infection-induced pop-up ads for programs (such as Sysprotect and WinFixer) that claim to remove system vulnerabilities.

If you suspect other stubborn spyware infections remain, consider downloading and executing the following antimalware programs:

- ComboFix -- Detects a variety of malware infections.
- EZPCFix -- For Windows 2000/XP, helps clean a variety of malware infections.
- Microsoft's/Sysinternals' AutoRuns For Windows -- Similar to Trend Micro's Hijack This, AutoRuns for Windows provides a powerful utility for editing auto-starting programs and processes.
- Microsoft's/Sysinternals' Process Explorer -- Powerful utility that helps track which program opens a specific file or directory.
- Sunbelt Software's Counterspy -- Quite possibly the definitive spyware identification and removal application.
- Trend Micro Hijack This -- Powerful and widely used tool for identifying processes, programs, browser objects and registry entries that load at startup.

NOTES

- *When installing Spybot S&D, choose to install the TeaTimer system settings protection (with the SDHelper Internet Explorer protection) to help arrest rogue processes.*
- *Please recognize that many of the utilities listed in this section could potentially make damaging changes to Windows' installations.*
- *The Windows winsock stack can be reset at the command line using the command: netsh winsock reset.*

IV. Final steps

Once a system has been cleaned and rogue processes, DLLs, registry entries and unwanted programs have been removed or arrested, reboot the PC normally. Confirm that pop-up windows have been eliminated, browser sessions operate properly (with no Internet home page redirection) and network communications work as intended.

Next:

- ☑ Purchase a license for, download and install a business-class antispyware application (being sure to register the license and download updates immediately).
- ☑ Schedule regular (daily) updates and full-system scans.
- ☑ Periodically review scan and update logs to confirm the program is working as intended (and properly removing any found infections).

Among the effective antispyware programs to consider are:

- ➢ Lavasoft's Ad-Aware Pro.
- ➢ Sunbelt Software's Counterspy.
- ➢ Webroot Software's AntiSpyware or Spy Sweeper.

Also, consider an effective all-in-one (antivirus, antispyware and potentially antirootkit) solution. Effective options include:

- ➢ AVG Technologies' (formerly Grisoft) AVG Anti-Virus 8.0.
- ➢ Symantec's Norton AntiVirus 2008 With AntiSpyware.
- ➢ Webroot Software's AntiSpyware Corporate Edition with Antivirus.

Then re-enable Windows' System Restore and create a fresh restore point.

NOTES

- *Organizations should consider running a minimum of two antispyware applications on desktop PCs, particularly those at high risk of infection.*
- *All Windows systems should take advantage of Microsoft's free Defender software. While not effective as many other independent programs, IT professionals should at least load the program for minimal protection against known, widespread threats.*

Additional resources

- TechRepublic's Downloads RSS Feed XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Check out all of TechRepublic's free newsletters

Version history

Version: 1.0

Published: May 20, 2008

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to drop us a line and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team