

By Erik Eckel

1

2

Spyware has quickly outpaced viruses as a scourge to businesses. A 2005 FBI study revealed 79 percent of enterprise PCs in the United States are infected with spyware. Worse, according to a 2006 report by Radicati Group, each infestation costs businesses approximately \$265 when downtime and repair are factored in.

By deploying and maintaining effective anti-spyware tools, organizations can protect themselves from lost productivity and potential data loss resulting from spyware infestation. Here are 10 things to look for when selecting an anti-spyware platform.

A potent anti-spyware engine

An anti-spyware application is only as good as its signatures database. The application's underlying anti-spyware engine must be comprehensive. Offerings from leading vendors track as many as three-quarters of a million potential infections, so it's critical that the application you select has a sizable and potent anti-spyware database.

Automatic updates

h. 🍳 🖉 🕷	
Status Update Scanner Shield Infections	Reports Analysis Tools Help
▽ Current Status	▽ Settings
Downloading updates, receive data	If you need to use a proxy to connect to the
	Internet, you can specify it below, otherwise you should not modify these options
- Hannahan lat	
▽ Manual update	Use proxy
Here you can manually run an update. We recommend using the automatic update to always be protected against the latest threats.	Туре: НТТР
	Host: localhost
Please wait	Port: 8080
▽ Automatic update	
 Automatic update Download and install updates automatically (recommended) 	Authenticate on proxy
	User:
Here you can set up the automatic updates time interval. This feature is only available for paying customers.	Password:
Show notification when an update is installed automatically	1 asswolu.
Update interval: 60 minutes 💌	

The best anti-spyware programs support downloading updates automatically.

staff member, maintaining a PC's anti-spyware database isn't included in their job description. So anti-spyware programs aren't likely to remain current unless the feature's built into the software application itself. Insist on an anti-spyware application featuring automated updates.

You should also er that the anti-spywa application you sel updates automatica New spyware and forms of malicious software are releas into the wild almost Quality anti-spywa manufacturers continually update code. Without thos updates, anti-spyw applications quickly become outdated a subsequently, ineff

Most every anti-spyware program includes access to updates. Some, however, require that users manually download and apply them. In busy organizations, users have other responsibilities. Unless

the employee is an IT

Active protection

3

4

5

Some anti-spyware applications remove spyware infestations found only while conducting manual scans. To best prevent spyware from infecting a system in the first place, seek an anti-spyware program that includes active protection. By actively monitoring system, process, and network activity, a capable anti-spyware application can block malicious software from installing in the first place.

There's no sense in waiting for a manually triggered scan to identify performance-robbing spyware and then have to remove it. Preventing the infection via active monitoring processes is by far the preferred option.

Customizable scans

Look for an anti-spyware program that lets you schedule customizable scans. Different workstations are used for different purposes. Based on their intended use, some systems will benefit from more thorough anti-spyware scans. However, the anti-spyware program must support creating the customizable scans.

For example, systems frequently used for Internet browsing may well benefit from daily scheduled anti-spyware scans that check active memory, the Windows registry, the Windows directory, cookie folders, and all hard drives for infestation. On the other hand, systems rarely used for Internet browsing may require only weekly scans of their hard drives.

Seek an anti-spyware program that includes such flexible scanning features.

#Unattended capabilities

Standardize on an antispyware utility that permits unattended maintenance and administration. The ability to schedule unattended updates and scans ensures that the program you deploy provides effective coverage and protection.

Users typically require access to their desktops throughout the entire business day. So there's little time for technical support staff to interrupt users' work for purposes of updating and scanning systems, especially when a thorough scan of a large hard drive can require more than an hour to complete. Neither do IT staffs have time to visit each workstation within

	AVG Anti-Sp	yware							_ 🗆 🗙
	Do Status	COLUDIE Update	Scanner	Shield	Infections	Reports	Analysis	Tools	Help
_	Scan		Settings	Scheduler					
	Profiles		Scheduled	🗹 Schedule th	is profile				
	3 New Profile1		Yes	Start time:			05:00		
					◯ Time afl	ter startup	05:00	**	
				Period:	Every 2nd	I Day 🔽]		
				☐ Don't exe ▽ Executi Last tim	cute if a fulls on statistics e executed neduled sta	: I: Friday, D	tion is running December 22, 2 December 24,	as possible (e.g. a game) 2006 5:00 AM ,2006 5:00 AN	

Good anti-spyware programs can schedule unattended anti-spyware scans (during off hours).

the organization to manually configure updates or execute anti-spyware scans.

Scheduling unattended updates and thorough system scans during off hours, when no staff are present, helps optimize administrative time and productivity.

Effective quarantining/containment

When unattended scans are configured, it's critical that the anti-spyware application effectively quarantine infections that are found without requiring user interaction. Unless the anti-spyware program can contain active spyware and remove infections automatically, the application will essentially prove useless in business environments.

Process monitoring

Spyware and adware programs exist in so many iterations and derivatives that it's often difficult for even the best-built antispyware programs to catch every form of malicious software. However, anti-spyware tools can go a long way toward helping technology administrators track down and eliminate malicious software not yet identified or recognized as spyware.

6

7

By including a process monitoring utility within the anti-spyware application, software manufacturers can simplify the task of identifying and eliminating unwanted software. Although many spyware programs hide themselves from Windows Task Manager,

8

h 🍳	20		*	Ů			?
Status Update	e Scanner	Shield	Infections Reports	Analy	sis	Tools	Help
Processes	Connections	Autostart	Browser Plugi	ns	LSP View	ver	
	D-14		Window	T-1	Constan	DID	
rocess name	Path		WINDOW	Internet	Service	PID	~
AgentSrv.EXE	C:\Program Files\Ren			Yes	Yes	1284	
ALCWZRD.EXE	C:\WINDOWS\ALCW			No	No	1356	_
alg.exe	C:\WINDOWS\\$ystem32\alg.exe C:\Program Files\APC\APC Power C:\WINDOWS\\$ystem32\Ati2evx C:\WINDOWS\\$ystem32\Ati2evx C:\Program Files\ATI Technologie C:\Program Files\Grisoft\AVG7\avg C:\Program Files\Grisoft\AVG7\avg C:\Program Files\Grisoft\AVG7\avg C:\Program Files\Remote Data Ba C:\Program Files\Remote Data Ba C:\WINDOWS\\$ystem32\csrss.exe C:\WINDOWS\\$ystem32\dlhost.exe C:\WINDOWS\\$ystem32\dlhost.exe			Yes	Yes	2336	=
apcsystray.exe				No	No	2132	
Ati2evxx.exe				No	Yes	1672	
Ati2evxx.exe			AVG Anti-Spyware 7.5	No	No	2036	
atiptaxx.exe				No	No	2924	
avgamsvr.exe				Yes	Yes	1380	
avgas.exe				Yes	No	1116	
avgcc.exe				No	No	864	
avgupsvc.exe				No	Yes	1404	
brctrcen.exe				No	No	3696	
CBSysTray.exe				No	No	2492	
csrss.exe				No	No	1400	
Csrss.exe				No	No Val	3104	
dllhost.exe				Yes	Yes	544	
DvzIncMsgr.exe				Yes	No	2128	
"ehmsas.exe "ehRec.exe	C:\WINDOWS\eHome\ehmsas.exe C:\WINDOWS\eHome\ehRec.exe			No Yes	No No	4020 4468	~

AVG's Anti-Spyware 7.5 includes a potent process monitoring menu from which administrators can terminate unwanted processes.

better anti-spyware programs include process monitoring features enabling support staff to track and eliminate malicious software Windows itself doesn't see.

Autostart monitoring

Along with providing support for monitoring active processes, anti-spyware applications should monitor programs that start automatically when Windows loads.

Spyware programs have become fairly sophisticated. Few appear within Control Panel's Add/Remove Programs applet, and fewer still install within the Start | All Programs menu's Startup folder. Thus, administrators require a potent anti-spyware program capable of monitoring programs that load automatically at Windows startup. Look for an anti-spyware program that includes autostart monitoring, thereby simplifying the process of removing unwanted software and blocking spyware from loading when Windows starts.

Centralized administration

As mentioned in #5, technology administrators (particularly those in larger organizations) don't have time to manually administer or support each individual workstation. It's impractical for many technology staffs to attempt visiting each workstation in person to ensure anti-spyware engine updates are in place, scans are completing as scheduled, and infestations are being quarantined properly.

9

In larger organizations, look for an antispyware application that includes a centralized administration console. Such products are often exponentially more expensive than their non-centralized administration-capable counterparts, but the time saved will more than make up the difference within busy IT departments.

Spy Sweepe	r [™] Enterprise				User: admin (Logout
Webroot Enterprise Dashboard	Client Install / Uninst Network View Name / IP	Status	Name A	Version	Last Heartbeat	•
Server Status			SONYVAIO			
License Status			XPTEST	3.1.0.1844	5/11/07 12:07:09 PM	
 Client Management Sweep Now Client Install / Uninstall Distributors User Management Configuration Updates Notification Management Reports Spyware Trend by Type Top Threats Spyware Detail Infected Machine Summary Spyware Detail Spyware History Version History Fror Report News and Docs 						
	To install or uninstall clients, you r Admin Console service. This is do see the System Administrator Guit	nust first pro	e Windows Services	dentials of a Dom		

Webroot's Spy Sweeper Enterprise has a wide range of centralized administration features. In addition to installing the anti-spyware software on systems throughout the organization, it enables remotely tracking errors, conducting sweeps (or scans), configuring updates and more.

10 Quality reporting

Anti-spyware applications must include effective reporting capabilities. In addition to listing whether scans complete properly, good anti-spyware programs will track infestations that are found, the results of quarantine efforts, and confirmation that updates were downloaded and applied properly.

Additional resources

- TechRepublic's <u>Downloads RSS Feed</u> XML
- Sign up for TechRepublic's Downloads Weekly Update newsletter
- Sign up for our <u>IT Management NetNote</u>
- Check out all of TechRepublic's <u>free newsletters</u>
- 10 things you should know about fighting spyware in Windows XP (TechRepublic download)
- <u>Windows Defender in Vista offers built-in spyware protection</u> (TechRepublic download)
- Combat spyware in your enterprise with these forensic tools and techniques (TechRepublic download)

Version history

Version: 1.0 Published: June 20, 2007

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 <u>drop us a line</u> and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

-The TechRepublic Downloads Team