Protect Your PC: General Information, and a Specific Approach

Dave Ihnat
dihnat@dminet.com

December 14, 2004
Updated January 23, 2007

---

1. INTRODUCTION

Computers, both personal and business, are under increasing attack from both traditional and new software threats. This memorandum recommends a general approach to protect a workstation or small server, and specific software and procedures.

It is deliberately written in an extremely informal, sometimes chatty style. If that isn't acceptable, please feel free to search the Internet for a graduate thesis somewhere.

The most recent version of this document may be found on my website at:

http://www.dminet.com/papers/Personal_Computer_Protection.pdf

2. OVERVIEW

Malware—a term for malicious software, including "traditional" viruses, Trojans, and worms, as well as newer threats such as spyware and adware—has burgeoned in the last year. An increasing number of business and home computers are falling victim to this growing scourge; some infestations are so virulent that some people find it easier to buy a new computer than spend the time and effort to recover the old software installation!

This memorandum provides a little insight into how these things work, what they do, why they exist, and recommends a specific set of software and procedures to help protect a computer at this particular point in time. The "right" software to attack these invaders changes almost monthly, but the general approach will remain valid as long as the underlying system architectures remain the same.

2.1 I DON'T CARE—I JUST WANT TO *DO* SOMETHING

Ok, you don't need to read all the history and explanation. Do this:

1. Go to ***Section 5*** for specific recommendations of what to buy or download.
2. Install all of the hardware and software, following the vendor or software's instructions.
3. Go to ***Section 6*** every week or two, and follow the steps detailed there. There are a lot of pictures and "click here" instructions.

2.2 TARGET MACHINES

The general approach, and all of the specific solutions discussed, are Microsoft Windows-specific. There is a good reason for this: Windows is the most vulnerable platform in wide use today. If you've another platform, the common thread is to use a good firewall; and if you serve

files to Windows machines, try to provide an Anti-Virus (AV)/Anti-Spyware (AS)/Anti-Adware (AA) solution to your clients.

You may ask, why is Windows so vulnerable? This is a complex topic, hotly disputed by Microsoft. The consensus is that, simply put, security was never important to Microsoft when developing first MS-DOS, then Windows. Their primary focus was on making everything *simple*—simple to use, simple to develop for. (Whether they succeeded is yet another hotly debated topic.)

Mechanisms for making machines much more resistant to infiltration and corruption were well understood by the time Microsoft flooded the world with MS-DOS; failure to design such fundamentals into the software at that time was a matter of design philosophy, not due to a lack of knowledge. Only in the last several years has Microsoft even made a strong verbal commitment to tightening its products against infiltration and providing tighter security. Many people believe it's too late—that there are literally billions of lines of code, hundreds of products, and all designed without security as a basic goal. The argument is that nobody, even Microsoft, has enough time, money, and people to actually review, redesign, and fix all that code. I suppose we'll see in the next few years…

2.3 TARGET AUDIENCE

This paper is intended for the casual computer user. If you're already a comp jock ("power user"), you're probably reading it just to laugh and point out omissions or (what *you* think are) errors. But the goal is to teach uninformed computer owners and users about these dangers; and to tell them enough about how to protect themselves to offer a reasonable barrier to the unchecked spread of malware.

As such, it also is targeting the home user; home office user; or small business user. One to several machines, with some sort of broadband Internet connection—DSL or Cable, usually. And no Information Technology (IT) staff to protect them.

So if you're reading this and, especially, if there's some cool download you really, really want to run—and you aren't sure if it's going to be safe or not—it won't help you; my answer here will be "don't do it if you don't know". My advice, if you need a quick answer, is to ask someone who does know about this stuff.

It's my hope that this paper will prompt you to do some studying and research such that you grow beyond the 'cookbook' protections I describe here.

2.4 USAGE

If all you want to do is find out what to do to protect your machine, skip all of Section 3. It's mostly background and description to let those who are interested understand what all this is about. "Know Thy Enemy", so to speak.

Section 4 discusses the general class of protection approaches that seem to help keep this mess in line; if you just want cookbook solutions, skip this, too.

Section 5 specifically recommends software, where to get it, and how to run it. Some people might say, "Finally! After all the claptrap…"

3. MALWARE

What *is* "malware"? Just what does it do? And why do people *do* this?

3.1 WHAT IS MALWARE?

Malware is an abbreviation for *Mal*icious Soft*ware*. Malware is a fairly recent term. Generally, until the last few years, people referred to specific, common types of malevolent software—viruses, worms, or Trojans. Now, they include the general class of software referred to as AdWare or SpyWare.

3.1.1 "Traditional" Malware

No matter the target system, be it Windows, Unix, Macintosh, whatever, the general categories of "traditional" malware are:

- *Virus*. A piece of executable computer code that somehow injected itself into an already existing, valid program on a computer.
- *Worm*. A program in its own right that makes use of some discovered flaw in the target computer's security that allows it to copy itself onto that computer, assume privileged status (if the system supports such a concept), and then search for other connected systems it can infect.
- *Trojan*. A program that relies on a user to do something for it—for instance, click on an E-mail attachment to activate it—that permits it to begin execution. This is the most common initial vector today, as E-mail messages always seem to hook someone into clicking on that alleged picture of Martina.

Each of these terms describe the distribution mechanism. Worse, hybrids are common today—what may start out as a Trojan, attached to an E-mail message, will then start acting like a worm once it's on a system.

But another part of the software--the *payload*—is critical, as well. What the purpose of the software may be, beyond just copying itself to different programs and/or computers, is up to the author. Many are harmless—either no payload, because the whole purpose is to see if the distribution mechanism works—or pranks, such as printing messages. But far too many are malicious—triggering worm or virus activity, deleting files, reformatting disks, or, in modern incarnations, taking control of networked computers for remote access and use by the author or others. A relatively new, nasty, and totally unwelcome variation of malware is the *rootkit*. It essentially replaces parts of the operating system with its own components; an attack made easier by the model of the Microsoft operating system (but, unfortunately, not unique to Microsoft). The replacement component(s) generally carry out just the same tasks as the legitimate ones they replace—except they hide and protect the payload.

3.1.1.1 Building Better Watchdogs…Again, and Again, and Again

Traditional anti-virus companies have focused on detection and removal of this class of malware, including both its manifestations on disk, and that running in the computer's memory, through the use of *signatures*—unique patterns of code or text in the malware itself that their *engine* can recognize when given a list of such signatures.

Unfortunately, this approach means that some poor user (usually more than one) "in the field" has to be the sacrificial lamb—they catch a new "critter" and suffer whatever it's going to do to them. The cycle from that point, for virtually all of the anti-virus companies, is as follows:

- The anti-virus company then receives a report from this victim (and others like him/her) that the software can't identify this new threat.
- The company solicits an example from the victim(s), dissect and analyze it, and when they believe they understand the thread and how to correct it, incorporate the new virus "signature" and the correction into their products.
- They then expect—require, actually—their products on all client sites to be able to get to the company's update site and download these updates to protect all those who haven't yet fallen prey.

Worse, this has sparked an "arms race". The malware authors see a new challenge in creating software that tries to hide from these snuffling watchdogs—so-called "stealth" viruses, etc., that use some amazingly complex and adaptable mechanisms to "morph", or change, their signatures on-the-fly. The anti-virus companies analyze these, and virtually always come up with counter-measures. Which triggers new versions…

Moreover, two other developments have made this a losing proposition for the anti-virus vendors. First, not every would-be malware distributor need be a crack coder any more. The very good ones have written actual kits which their less skilled cousins—the ones we call "script kiddies"—just have to know how to run to generate a new variant on a virus, or a new payload. This means that, while each of these variants is usually not unique enough to stop the scanners from catching them, it redoubles the *number* of these things being distributed.

And worst of all, the Internet has permitted these guys to communicate quickly and anonymously, to spread new ideas and techniques, and to spread the word about new flaws discovered in operating systems that allow them a foothold for new malware. They used to talk about a week between a discovered flaw and an exploit; then it was days; then a day. Today, it's "Zero-Day exploits"; the very same day that the "White Hats" know about a flaw, the "Black Hats" have a piece of malware ready to exploit it.

3.1.2 AdWare and SpyWare

In the last few years, two new types of malware have become prevalent. Commonly called *AdWare* or *SpyWare*, these two categories of software have distinct goals:

- *AdWare*. Delivery of commercial advertising material. They use techniques such as hijacking the browser's home page to an advertising site; or bypassing popup blockers to download and display advertising.
- *SpyWare*. Usually not malicious in the "take-over-your-computer" sense (although these are showing up, too!). Rather, they want to know *where* you go, *what* you buy, *what* you are interested in.

As such, these things usually are very small, and really try not to damage your computer while carrying out their tasks. But at the same time, they go to great lengths to prevent removal; and many are, frankly, sloppy and buggy. Even if they don't have flaws, in the same way that a dog can tolerate a few ticks, but will sicken and die if infested with hundreds, these little bits of malware are causing machines to become unusably slow or even crash, since there's no limit on how *many* of these things will infest a computer. The most the author has removed from any one

computer was over 950; but virtually any Windows-based computer today that's connected to the Internet will, when scanned, yield at least 50 or 60.

3.1.2.1 How Are They Transmitted?

Although incorporated in "legitimate" software as a ruse to get in the door, these are quite often transmitted through flaws in web browsers—and the most commonly exploited browser is Internet Explorer, or IE. (Why? Go see *Target Machines*.)[1]

But what was that about "legitimate" software? Yep. Some of them attempt to wear the trappings of real, licensed software. They may work a deal with your Internet Service Provider to be included in their software packages, with "licenses" in all the legal mumbo-jumbo that users never seem to read. Or they may be buried deep in a web site's "Acceptable Use" policies, and piggybacked on/buried in something users like, such as WeatherBug, or especially "Peer-to-Peer" (P2P) software such as LimeWire, Morpheus, Kazaa, etc. Or cool, free downloads like games or screensavers.

So how do you avoid *these?* Well, one thing is to avoid what some call the "Dark Alleys" of the Internet—porn and gambling sites rank high on this list. Before downloading something that isn't totally mainstream—that is, either commercially provided by a verifiable vendor, or a well-recognized Open Source or freeware product—check to see if it's been identified as spy/malware; as was recently pointed out in a vendor's mailing (Thanks, WatchGuard!), take a look at Spyware-Guide's (http://www.spywareguide.com) or SpyChecker's (http://camtech2000.net/Pages/SpyChaser.html) lists of known spyware. Stay away from P2P software unless you really, *really* know what's going on under the sheets.

3.1.2.2 And Why Doesn't My Commercial Anti-Virus Package Kill Them?

This has caused problems for traditional anti-virus companies. Because unlike traditional authors of viruses, worms, and Trojans, many of these have companies behind them. Companies that have threatened legal action against anti-virus companies if they identify them as malware. Because of this legal danger, most anti-virus companies are moving very slowly in deciding how to address this problem—meaning that your copy of Symantec, or McAfee, or whatever, probably doesn't catch any of these.

3.1.2.3 So What DOES Kill Them?

Fortunately, the same movement that spawned Shareware and Open Source projects such as Linux has also provided a forum for Anti-Adware/Anti-Spyware (AA/AS) software. Usually free for home use, and either free or very inexpensive for commercial use, there is a plethora of tools available on the Internet to attack these critters.

---

[1] In fact, this is so demonstrably true that many experts are recommending that companies and individuals actually *stop using IE*. There are many excellent and either free or very inexpensive web browsers available on the Internet; a very good options are *Mozilla* (www.mozilla.com), which in addition to a built-in popup blocker and other security and utility features, also provides a mail reader and web page authoring tool; and *Firefox* (again, www.mozilla.com), which is just a browser (I recommend this if you don't need all the other programs). Another very popular browser is *Opera* (www.opera.com), which also has many added features but does cost about $39 USD.

3.2 WHO DOES THIS? WHY???

A common question that's asked is "WHY do people do this? Why do they want to crash MY computer?"

In the case of the newer malware—AdWare and SpyWare—the answer has already been given. It's quite commonly commercial in nature. Reprehensible, yes; understandable, yes.

But what about the older stuff—viruses, worms, Trojans? Why spend so much work and time on them?

Some of it has been academic in nature—"Gee, I just figured out that if you do *this*, then *that*, this program should infect every Unix computer in the world. Hmm…I wonder if it really works…" (This, roughly speaking, was the genesis of the Morris worm back in the late '80s. Oh, that one was followed by "Oops. Uh-oh…")

Some is geek adolescent "see how good *I* am" bragging rights. Some studies have shown that the typical cracker[1] ranges from about 12 through 30; is usually male; and has, on average, a high-school education. This sounds harmless, but can get pretty nasty, since one of the things that are prized are collected information, cracked commercial software ("Warez"), and someplace to store and distribute all this. There is a lot of competition in this circle—there are strong indications that one of the rounds of competing viruses earlier this year was a sort of underground war between two groups of virus authors.

But a really dirty edge has been brought to the arena with the prevalence—and economic incentive—of spam. There is now little doubt in security communities, with excellent data to back this belief, that organized crime, especially based in Eastern Europe and/or Russia, is paying crackers to come up with malware to take over computers that are Internet-connected. These machines have "back doors" installed that allow remote control and software installation, including mass-mailing programs. Then the "keys"—address and access credentials—to these compromised machines are turned over to the criminal organization, which can then sell hundreds or thousands of these compromised machines to large-scale spammers. The most sophisticated attack at the time of authorship is a truly scary creature—it incorporates its own anti-virus scanner (stolen and cracked from Kaspersky) to get rid of other viruses on the victim's machine—don't want to share the resources, now, do we?—and a complicated structure of communications with other "owned" machines and controller machines to manage the entire cracker-owned network.[2]

As of the last few months of 2005, another nasty edge has been added. Rather than pushing pills or porn, the spammers are pushing stock "pump and dump" schemes. And they're using

---

[1] And Please—it *is* cracker, not Hacker. A hacker is a skilled programmer, one who knows how to use the characteristics of a system or software to produce elegant solutions to problems. We in the community are quite miffed that the popular press didn't catch on to the distinction long ago.

[2] Michael R. Wayne, a friend of mine, added this exciting update on 25 February 2005:

> The *bad guys* have recently discovered a new commercial use for compromised machines. Once they have cracked your machine, they download a program that converts your box into a web server, running on a normally unused port. A centralized software package then adds your machine address into its list, downloads files to the box and uses **your** bandwidth to serve (sometimes illegal) pornography to **paying** customers around the world.

sophisticated techniques to hide the spam in pictures, rather than text. While anti-spam methods are beyond the scope of this document, the important point is that they rely on taking over millions of computers to *send* this spam—and if you're unprotected, you're a prime candidate to "donate" your machine to their cause.

4. PROTECTION: GENERAL APPROACH

The general approach is to:

- KEEP the bad guys out
- STOP them from getting back out if they get in
- CATCH and SQUASH them if they get in
- RECOVER if they win

And, of course, all on as small a budget as can be managed.

4.1 FIREWALL

A firewall is literally a barrier between computer communications within and without a private network. It consists of dedicated hardware and firmware that examines every packet of information that is directed into or out of the local network (or single computer), applying rules for acceptance or rejection. A firewall helps both to keep the bad guys out, and to keep them bottled up if they do get in.[1]

There are two types of firewall available to the small system owner: a hardware appliance, and a software firewall.

4.1.1 Hardware Appliance

The term "hardware appliance" has come to be used to describe the self-contained, compact, and largely plug-and-go devices that have become both common and affordable since the advent of widely available broadband services such as DSL and Cable. It's intended to convey their fundamental nature—they aren't highly customizable and programmable, as are "traditional" firewalls. But then, they don't cost $10,000, as traditional firewalls did (and do).

While it is generally unwise to just trust the settings on any security device as shipped to you—for one thing, if you know the default passwords and settings, rest assured the crackers do, too!—these usually can be installed by the relatively uninitiated without much trouble, and after installation, they tend to just run. It's not too far to go to say that *anyone* who has a broadband connection should get a hardware firewall. In fact, that's exactly what we are going to say.

However, even though they are resistant to general attack from outside, especially since their software is stored in a (usually) unmodifiable form in "firmware", they can have bugs. It's a good

[1] It gets its name from the fire-resistant barrier that cars have between the engine compartment and the passenger compartment—literally, in that case, a wall against an engine compartment fire and the cookable passengers in the vehicle. In the same way, a firewall stands between the "dirty" world outside your network, and your precious data and computers in your home or office.

idea to check the version of the firmware in your firewall periodically against the version on the vendor's website.

4.1.2 Software Firewall

A software firewall is exactly that—a program installed on your computer that, instead of having dedicated hardware on which to run, uses your computer's hardware. It injects itself into the communications between that computer and either the outside world, or the rest of the internal network, examining all program requests to send or receive data.

There are three general scenarios that call for using a software firewall:

- If the computer uses only dialup connections to the Internet, or is used at public access points (e.g., public library, hotel, or Starbuck's wireless access), a software firewall may be the only way to incorporate a firewall into the link.
- If the computer is the only machine to use a DSL or Cable connection, and for some reason a hardware firewall appliance can't be used.
- If a computer is part of a local network, probably behind a hardware firewall, but is particularly vulnerable to infection for some reason—for instance, a machine commonly used as a kid's Instant Messaging and Gaming system. In this case, the software firewall can help isolate other machines on the local network in case this machine gets infected.

While Microsoft Windows 2000 and XP, especially as of XP Service Pack 2, tout their built-in firewall capabilities, most professionals still consider these marginal and recommend a third-party firewall package. Particularly for home use, these can be found free of charge on the Internet.

The best solution is a "suspenders and belt" approach—use *both* a hardware firewall whenever you can, and in addition a software firewall running on the local computer. Incidentally, some people may comment to you that "it has been shown that malicious crackers can circumvent a software firewall once they gain administrative rights on your computer", with the implication that you it's not worth bothering. My only answer is that "it has been shown that some safe crackers can circumvent the combination locks on bank vaults." Despite this fact, I don't see banks leaving their vaults unlocked

A decent software firewall provides a noticeable degree of protection against many attacks; enough so that it's worth including, despite the fact that *some* may have vulnerabilities, and there may be *some* attacks that work against them. Defense in depth is a rallying cry in security—suspenders and belts, hardware and software protection.

4.2 CHANGE TARGETS!

Microsoft is *the* target of a legion of crackers. Once they can get into a system, Windows itself is a prime target of attack; a sticky point for the black hats is how to get into the system in the first place. "Outward-looking" utilities—programs that, necessarily, must talk to the outside world—are a logical point of attack, and of these, the two most common victims are Internet Explorer and Microsoft Outlook or Outlook Express. So why not just not use them?

In the following, it is understood that sometimes you simply *can't* decide to change programs. Perhaps your company mandates use of IE or Outlook; or maybe you don't feel comfortable

enough with computers to make such a shift in your usage. But if it *is* possible, please consider this as another layer in the defenses.

4.2.1 Change Browsers

Everyone uses Internet Explorer ("IE"). Unfortunately, the bad guys know this, too. They also know that Microsoft has never yet considered security as highly as they've considered nifty features; consequently, Internet Explorer is a huge, complex program that all-too-often exposes the user to security violations that crackers just love to exploit. Nobody knows exactly how many different malware exploits make use of holes in IE—but there are warnings and patches on an almost daily basis. Many computer security professionals have actually come to the conclusion that it's better to replace use of Internet Explorer with an alternate browser whenever possible.

Three prime candidates for use under Windows are *Mozilla* (the original full suite of Internet applications from Mozilla, now renamed "Seamonkey") and the browser-only offering *FireFox*—probably what most people should use (www.mozilla.com) —both free—and *Opera* (www.opera.com); not free, but inexpensive.

Aside from many modern features, including integral popup ad blocking, these browsers benefit from simply not being the target of every cracker on the planet.

But what, you may ask, about Internet Explore 7? Glad you asked. Late in 2006, Microsoft released its latest version of Internet Explorer, 7.0. There are a great many changes and increased security; that's the good news. There are a great many changes and increased security; that's the bad news. Basically, many, many websites—especially including banks and storefronts—simply aren't ready to work with the new IE, at least as of January 2007. So you *can* move to it—but it's highly likely that you'll find many sites broken.

Now, if you move to an alternative browser, you'll still have to keep IE around for those sites that are written for, and only for, IE; but those are becoming less common as time goes on. As a friend commented on reading this section,

> Note that there is nothing preventing you from using your alternative browser for 95% of your web surfing and reverting back it IE for the few sites that require it. This gives you an immediate advantage over most Internet users since you will **not** be using IE when you encounter a random, possibly hostile site.

4.2.2 Change E-Mail Clients

Many of the arguments for using a different browser apply to the Windows E-mail client. *Outlook Express*, or its big brother, *Microsoft Outlook*, are feature-rich mail clients. Unfortunately, "feature rich" can also be translated as, "can allow, unbelievably enough, execution of malicious code and attachments in E-mail from unknown senders". In recent updates, some of these vulnerable features have been turned off by default—but they can (and often are) turned back on by unsuspecting users who really *must* see that dancing hamster in their inbox.

Webmail clients—often offered directly from your ISP—or full replacements such as Mozilla's *Thunderbird* (www.mozilla.com) or *Eudora* (www.eudora.com), offer the benefit of not being the target of all those malicious coders, while still offering a rich set of features for the end user. (Thunderbird, although new, is especially promising.)

4.3 ANTI-SPYWARE/ANTI-ADWARE

As mentioned earlier, there is a plethora of software tools, many free for personal use, that target AdWare and SpyWare. Generally, these are of two types:

- *Inoculators*. Most AdWare and SpyWare tries to see if it's already been installed on a computer, so it doesn't waste its time infesting a machine it's already compromised. These tools attempt to leave false markers or indicators to convince the software that it's already got this one, so don't bother. Typically, these are only run once, when they install the markers, and only periodically afterward to check for updates that protect against newly discovered malware.
- *Scanners*. Scanners work exactly like traditional anti-virus packages, using signatures and active scans of the computer to identify installed malware. Some are developing additional protective mechanisms, such as auditing the system configuration (Registry database) for suspicious changes.

The general approach that has proven most useful is to run at least one inoculator, and to identify at least two different scanning packages that are highly recommended, and to install and run them sequentially. This is on the premise that, written by different authors, they look for different sets of malware. While there may be—should be!—significant overlap, there is enough difference that what one misses, the other should catch.

4.4 ANTI-VIRUS

The old and faithful standby—because most of the AS/AA software leaves the traditional malware to Anti-Virus scanners.

Unfortunately, one approach that's working well for AS/AA scanners isn't as widely applicable for anti-virus packages: running more than one on the same system, on the assumption that "what one misses…". These packages tend to interfere with each other—several, such as AntiVir, actually explicitly warn you to *not* run it with another anti-virus package.

Also, most are commercial and cost money. Fortunately, in the last couple of years some very decent scanners are available to individuals and even companies for free. For instance, ClamAV is an Open Source scanner that has dedicated adherents. It doesn't yet have some of the useful or simply pretty features of the commercial packages, but it *does* catch bugs. A good commercial scanner that's free for personal use is AntiVir.

4.5 BACKUP

Old but Gold: Backup your data, so even if the nastiest virus reformats your hard drive, you have a copy to recover from. This is harder to accomplish than it used to be, since tape drives—the traditional standby backup medium—remain slow, expensive, and are increasingly outstripped in capacity by gargantuan-but-cheap hard drives on the market.

There are at least two approaches available to the small systems owner. Given the presence of a broadband connection, and the trust that data will be protected in transit and storage, there are several companies offering off-site backup services. They will literally drain the data from your system over what they claim is a securely encrypted Internet connection ("tunnel"), and store it off-site for you.

The second alternative is to make use of these stupidly large, cheap hard drives that are available as removable hard drives for backups. The most common approach is to use external USB enclosures that allow Windows to deal with removal and installation of "IDE" or "SATA" disks without rebooting. One major advantage of a removable hard drive is that it *is* removable—if it's dismounted, it can't be infested. When you're not backing up, dismount and at least power it down.

Of course, given the backup hardware, you still need to find a software solution—something has to collect and move the data *to* and *from* that backup hardware. Current versions (e.g., Windows XP) of Windows come with a Backup utility that, while having issues (as most Microsoft software does), will work acceptably well for most home and even small business users.

There are also commercial versions of backup programs that are very cheap for home or single-workstation business users. Two that have gained the loyalty of users are *Acronis True Image* (directly from www.acronis.com, approx. $50USD), and *Dantz Retrospect Professional for Windows* (approx. $90USD street price; search for it via Froogle or shopper.cnet.com).[1]

5. SPECIFIC SOLUTIONS

This is what the impatient have been waiting for—skip the gab, What Do I Do Right Now?

These recommendations are very specifically the author's. Others may argue with me; fine, it's a free country (so far). But I'm writing this, so I get to say what I think is best.

5.1 FIREWALL

We can't say it often enough:

> **If you have a broadband connection—Cable or DSL—you must get a hardware firewall appliance.**

Your cable or DSL provider may have given you a "modem" that has firewall capabilities; that's fine, IF you can program it, and IF it provides adequate capabilities. If not, don't trust them—put in your own between their box and your computers.

5.1.1 Hardware Appliance

If you need **wireless**, either of the following devices are inexpensive and reliable[2]:

- *D-Link DI-524*. D-Link's entry version of the 802.11g and 802.11b firewall/router and 4-port switch. If buying from D-Link, this is the wireless unit to get. www.dlink.com for specs; search the Internet for prices.

---

[1] Retrospect is a "crossover" product that started in the Macintosh world; make sure you pick the right platform and version if you choose this!

[2] I do have to insert a caveat here. LinkSys was bought out by Cisco in 2003, and while I, personally, haven't had problems, some people have reported a perceived drop in reliability since then. A typical comment is one made by Eric S. Raymond in an E-mail (quoted with permission):

" I've stopped buying Linksys hardware. I used to like the stuff, but I had too many of their boxes go inexplicably dead on me. Quality control seemed to [decline drastically] after the Cisco takeover."

- *LinkSys WRT54G*. LinkSys' entry version of an 802.11g *and* 802.11b wireless firewall/router, and has a 4-port switch for the internal network. If you're buying a new unit, this would be the one to pick from LinkSys. www.linksys.com for specs; search the Internet for prices.

If you **don't** need wireless, again, either of these will serve well:

- *D-Link DI-604*. Basic firewall/router and 4-port switch.
- *LinkSys BEFSR41*. LinkSys' venerable router/firewall and 4-port switch.

If you're not comfortable programming the device, get a friend to help. Even if it "just works" when you plug it in, you should change default settings, passwords, etc.

5.1.2 Software

5.1.2.1 Zone Alarm

ZoneAlarm Basic (www.zonealarm.com) is probably the most widely used software firewall on Windows, but that's mainly because it's free for personal use. The web site is confusing—they do a very good job of chivvying you to buy the commercial version, which, while not a bad product, is more than most people need.

5.1.2.2 Windows

This is being mentioned here because Microsoft is making quite a to-do about its built-in "firewall" in Windows XP and especially XP SP2. The bottom line is, at this point in time, turn it off and get ZoneAlarm.

5.2 ANTI-SPYWARE/ANTI-ADWARE

There are *many* of these; the combination recommended here is a personal preference just because, so far it seems to work well.

5.2.1 Ad Aware

Lavasoft's *AdAware Personal* is free for, as the name implies, personal use. www.lavasoftusa.com, again, watch out for the attempts to point you to the commercial version.

5.2.2 SpyBot S&D

This package recently incorporated a registry watcher called *Tea Timer*. Between that, and the basic scanner, this is a very good choice. http://www.safer-networking.org/en/download/

5.2.3 SpywareBlaster

This is an inoculator, and it's good enough that SpyBot knows about it and defers to it. www.wilderssecurity.net/spywareblaster.html.

5.3 ANTI-VIRUS

I'm going to assume you know about McAfee, Symantec, and Sophos. But if your scanner has expired, and you don't want to renew or buy one, the following are good choices.

5.3.1 AntiVir

This is probably the best free choice for the home user. It's available at http://www.free-av.com/; don't be put off by the fact that it's a German site, since they've done a good job translating (aside from the occasional virus warning that still pops up as *Achtung!*).

5.3.2 ClamAV

If you can't use AntiVir for some reason—say, you're a small business—or don't like it, the interface isn't as slick as the commercial versions, but the engine catches bugs. It comes from the Open Source and Linux crowd, and it shows—the Windows version is at the bottom of the download list. http://www.clamav.net

5.4 BACKUP

5.4.1 On-Line Backup Services

Frankly, I'm not going to get into recommending these. I haven't personally investigated them for security, reliability, and cost, and I'm somewhat twitchy about giving *my* data to someone else to safeguard. They should be simple enough to find by googling. Just make sure to check that they really *do* encrypt the data as it's going out to them (and coming back); that you really can recover; and that they do take care of your data while they hold it.

5.4.2 Removable Hard Drives

The best way to deal with a removable drive is to either buy a pre-assembled unit from a commercial vendor—they're quite cheap for drives in the range of 200-400Gb. If you're a bit more of a do-it-yourselfer, you can buy an external enclosure from vendors such as StarTech (http://www.startech.com) and then find the best deal on a hard drive to put into the enclosure.

5.4.3 Software

This is hard. Why? Because Microsoft Backup is, frankly, not great—but it's free on every system. Other backup solutions cost money—in some cases, a *lot* of money—and/or are complicated in strange and wonderful ways that make them unsuitable for a small-systems environment. And your backup software has to be something you trust—trust to work, trust to be portable, trust to be around long enough to support your backups. For all these reasons, selecting a backup solution should be done carefully.

5.4.4 Microsoft Backup

What can I say? It's free, it's there, it generally works. It doesn't know how to compress backups. It works for most people, so until you run out of drive space, or run into a problem it can't handle, why not.

5.4.5 Alternatives

There are *so* many to choose from. Many suffer from an overly-complex interface; others, an overly-expensive price tag. If you need one, find a tech friend and ask for help. Some candidates—google for where to find them—are:

- Acronis True Image (see above)

- Dantz Retrospect (see above)
- Genie Backup Manager
- NTI BackupNow!
- NovaStor NovaBackup
- Imaging software, such as *Norton Ghost* or *Powerquest Drive Image*. These make an actual copy of your entire disk to another disk that you can then simply store on a shelf.

6. PROCEDURES

Ok, this is the cook-book section; if you didn't want to read all the preceding stuff, you could just start from this point.

The assumption is that you have selected and installed:

- A LinkSys or D-Link router/firewall
- ZoneAlarm Basic
- LavaSoft AdAware
- SpyBot S&D with TeaTimer installed.
- SpywareBlaster
- AntiVir

I'm not going to assume that you got a removable hard drive, partly because if you did, there are too many different ways to configure it. If you decide to go that route, and get confused, ask a tech friend for some help dealing with *removable devices* and setting up your backup software.

Remember--when installing ZoneAlarm, be careful not to pick any of the "commercial" or "for pay" options.

Remember when installing LavaSoft, SpyBot, SpywareBlaster and AntiVir, take the defaults and if the installer suggests letting it do something, let it. In particular, Spybot has a component called *Tea Timer* that isn't checked by default. This is a very useful *resident* tool, meaning it remains in memory constantly watching the system. It audits a very specific part of the Windows operating system called the *Registry*; essentially, a special database of configuration options and installed programs. Virtually any piece of malware that wants to get anywhere on your system has to do so by creating one or more entries in the Registry. The Tea Timer simply watches for changes. It doesn't know if any change, in and of itself, is good or bad—it'll just let you know it's happening, and ask if it's OK to allow the change.

The simple rule to follow is:

- If you are installing or removing software, or doing something that might logically cause changes in Windows, like applying updates from Microsoft, these notices will pop up and are almost certainly because of what you're doing, so allow them.
- If you're just browsing along, or editing a document, or playing a game, and one of these alerts pops up, it probably *isn't* OK. Write the details down and call someone who knows about these things; if you can't immediately contact anyone who could tell you if the change is acceptable, don't allow it.

6.1 FIREWALL APPLIANCE

Make sure to set your passwords—read the manual. Every 3 months, look at the vendor web site to see if there's a new version of the firmware that applies to your device. They'll also have directions on how to download and install firmware updates. If you use a day planner or a PDA, actually enter this as a task on the first day of every quarter!

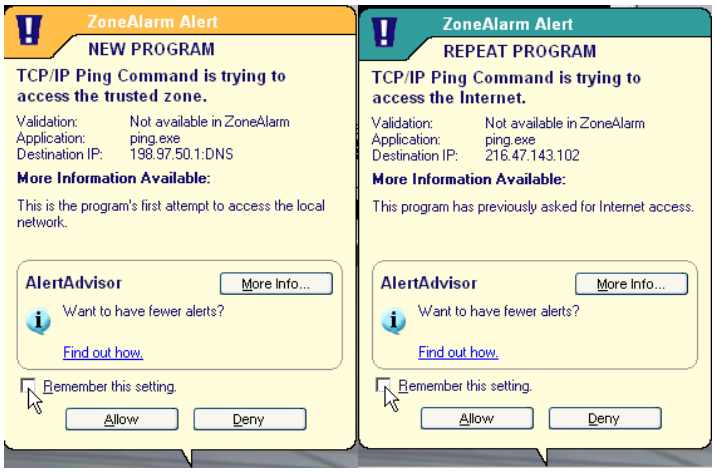
A special warning to DSL and some cable users. There is one particular configuration of service called *PPPoE* that's often used by Internet Service Providers (ISPs). All that's important for you to know at this point is that a *login* and *password* are required for PPPoE service; this is usually stored in software (usually buggy and slow software, too) provided by the ISP. All of the DSL/Cable firewall/switches recommended can handle the PPPoE login/password authentication—meaning you can uninstall the software that came with your service. But it also means that if you ever change the password for your service—usually the password for the main E-Mail account—*you have to remember to change it in the firewall setup*.

If you fail to do so, you'll probably work for anywhere from a day to even a couple of weeks, until the ISP resets your connection. And suddenly you won't have Internet service, because the wrong password is coded into your firewall, and you won't remember at this late date that you changed it. So I'm putting this here, in the section you're likely to review once every couple of weeks.

6.2 ZONEALARM BASIC

Let it check for updates when it asks to do so.

While working with your computer, ZoneAlarm will offer a popup when programs ask for Internet or local network access (usually both). An example of the two windows that will pop up (one after the other!) for the Windows *ping* command follows:



Don't just click "Deny" or "Allow"—if you don't know what the program asking for permission is, and what it does, write down its information—Command name, Validation, Application, and Destination IP—deny the request, and ask a knowledgeable friend.

If you *do* know what the program is, and always want it to be able to do what they're asking, click the *Remember this setting* box (pointed to in the examples).

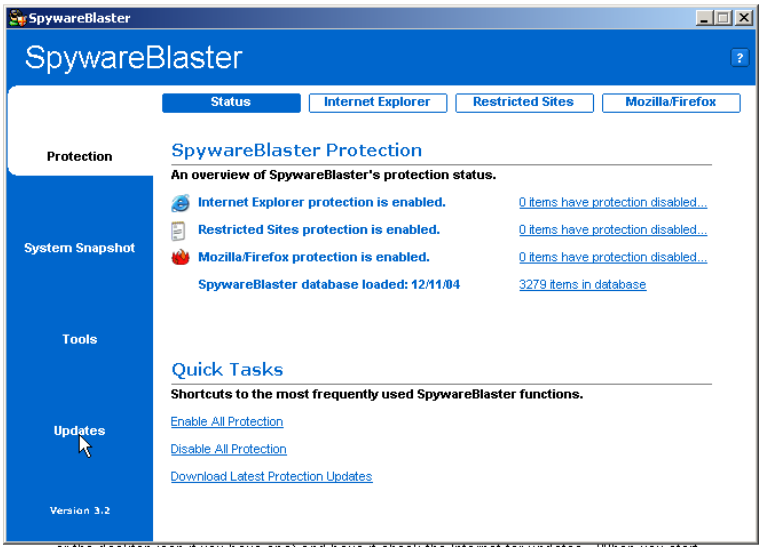
Once every couple of months, review the list of allowed/denied programs and make sure they all belong.

6.3 ANTI-SPYWARE

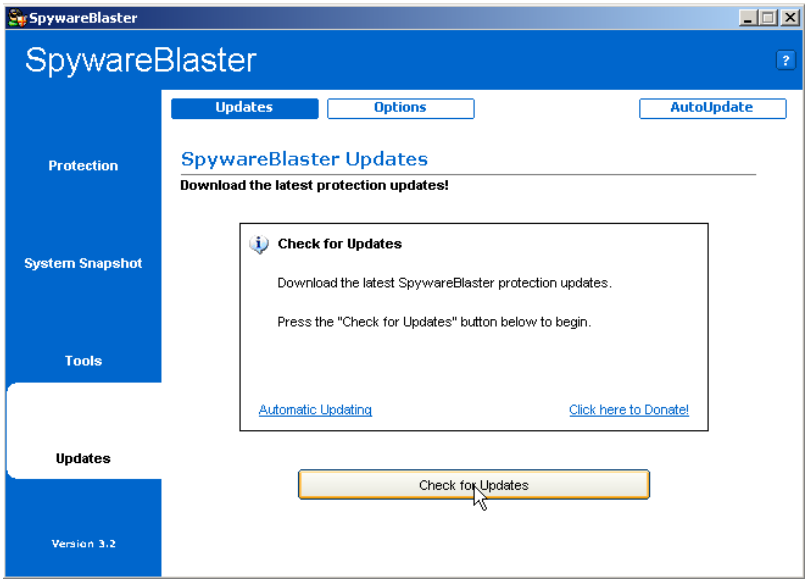
6.3.1 Spyware Blaster

Unfortunately, the free version doesn't automatically update.

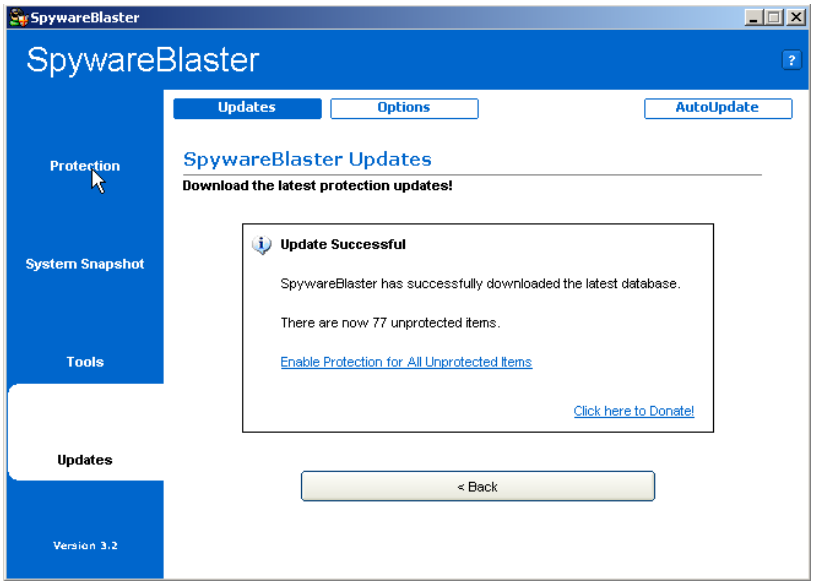
Once every 1-2 weeks, start the program (*Start->Programs->SpywareBlaster->SpywareBlaster,* or the desktop icon if you have one) and have it check the Internet for updates. When you start the program you'll click on *Updates*:



Then on *Check for Updates:*



If there is a new update, a number of dialogs will be displayed, ending with:



If anything was downloaded, make sure to click *Enable All Protection*..

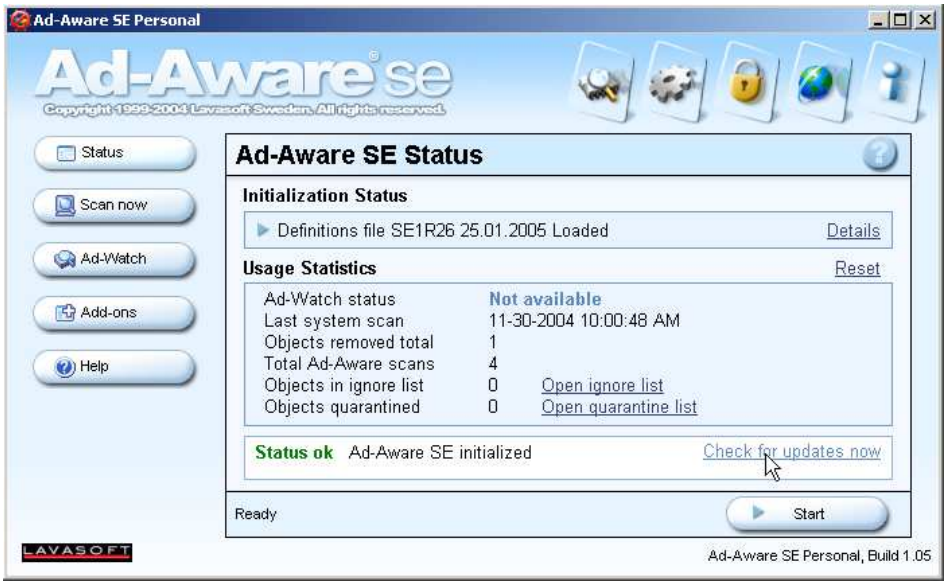
Since this is an inoculator, it doesn't need to be executed other than allowing downloads and applying unprotected items.

6.3.2 Lavasoft Ad-Aware

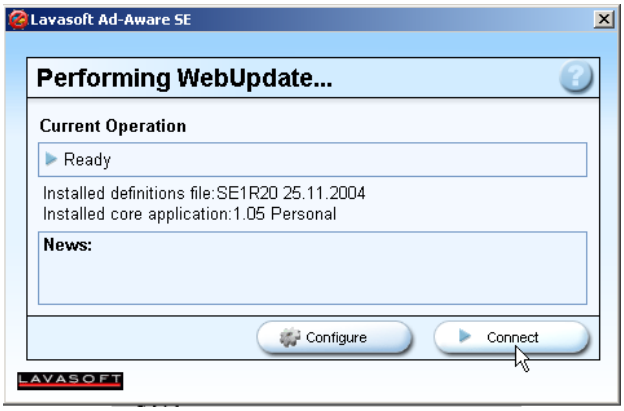
Unfortunately, the free version doesn't automatically update and can't be scheduled for automatic scans. (It doesn't cost much to buy, though.)

Once every 1-2 weeks, start the program and have it check the Internet for updates (*Start->Programs->LavaSoft AdAware SE Personal->AdAware SE Personal*, or the desktop icon if you have one.) It will probably pop up a window such as the following (hopefully without being quite so old):

If your definitions aren't quite as old, you may just get the main screen:

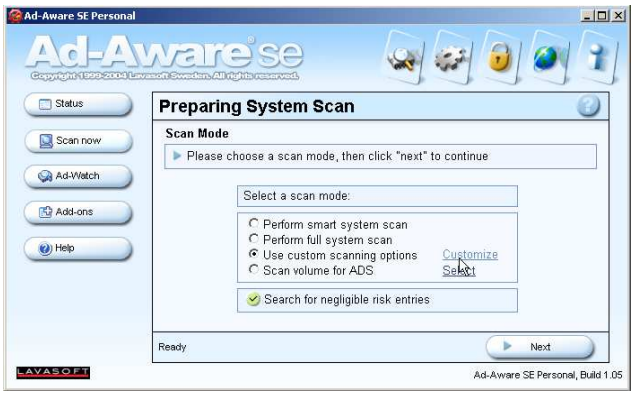


In this case, click on *Check for updates now*, as shown. In any case, after some setup, you'll get the following screen:

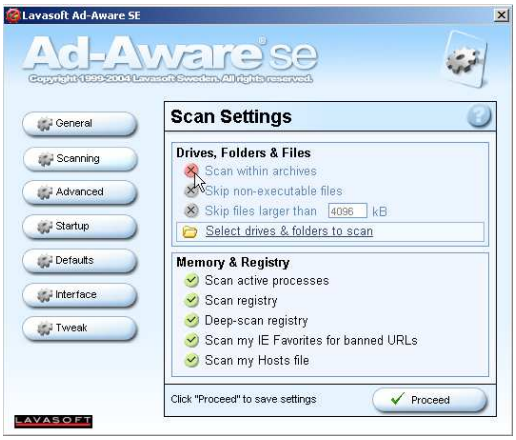


Go ahead and click on the *Connect* button. It will then try to check for new updates and, if it finds any, will ask if you want to download them. *Always* answer yes if it finds any! When done, the above box will change to let you know everything was transferred, and offer a *Finish* button. Click it to go to the Main Screen as shown above.

Whether or not anything was updated, you need to scan the system. Click on the *Start* button. You'll be presented with the following screen:

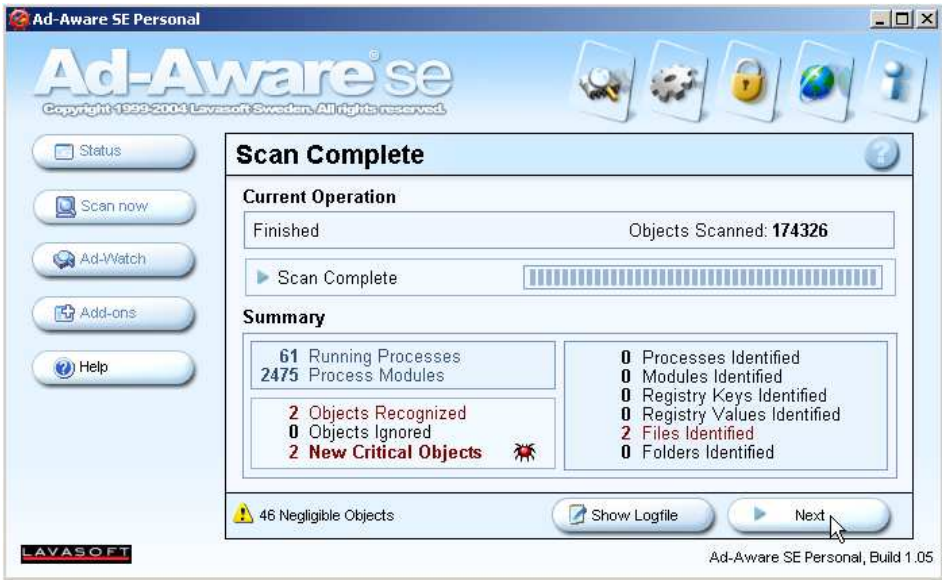


I recommend the *custom scanning options*. The first time you run AdAware, there is one option you want to set—after that, it'll be remembered. Click on the *Use custom scanning options* radio button—hightlighted above—and click on *Customize*:



Iif the *Scan within Archives* choice is off—as it is in this example—click it to turn it to a green checkmark. Then click the *Proceed* button.

If you've already set this option before, then just make sure *Use custom scanning options* is selected on the Main Screen and click on *Next.* The program will proceed to scan your computer—be patient, it'll take a few minutes. Hopefully, it won't find anything. But if it does, the screen will look something like this:



Go ahead and click on the *Next* button. If there are only a few objects found, you could click on each of them before getting rid of them; but often, there are more than 100 of these things! The easy way to simply select all of them is to place the mouse pointer in a blank area of the dialog box—just under the *Tracking* in this example, or on the same line and to the left if there are enough items to fill the box—and right-click once. You will get the pop-up menu shown in this example; highlight and left-click the choice *Select all objects*, as shown here:

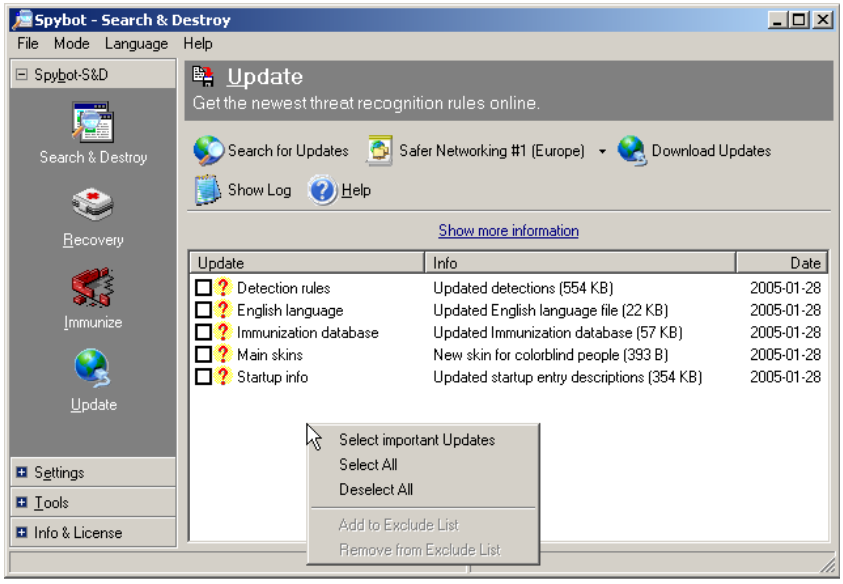
Once they're selected, click *Next*. It will tell you how many objects will be removed, and ask to continue; do so. Periodically, open the *quarantine list* and delete the archived items there.

6.3.3 Spybot S&D w/Tea Timer

Unfortunately, there doesn't appear to be any way to schedule an update. But it *does* allow you to schedule an automatic scan—look in *Settings* under *Scheduler*.

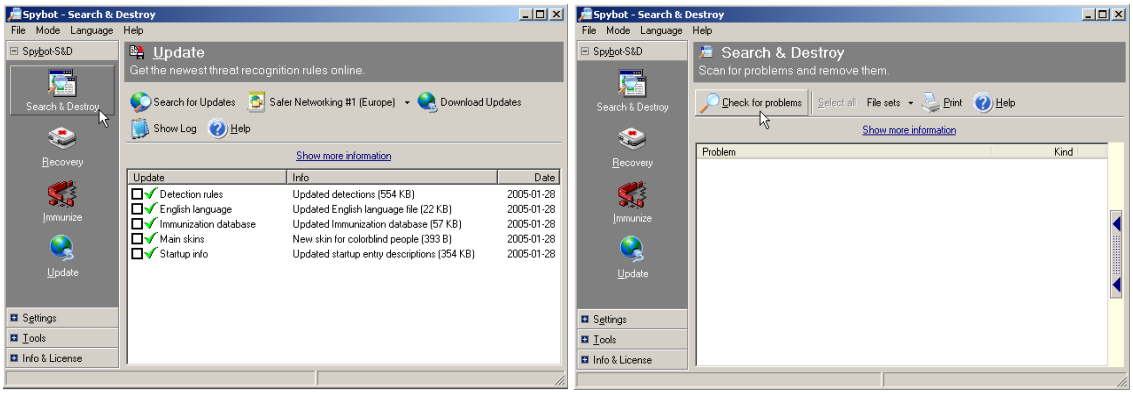
Once every 1-2 weeks, start the program (*Start->Programs->Spybot Search & Destroy->Spybot Search & Destroy*, or the desktop icon if you have one) and have it check the Internet for updates by, logically enough, clicking on *Search for Updates*:

It will check for updates, then display if any are available:

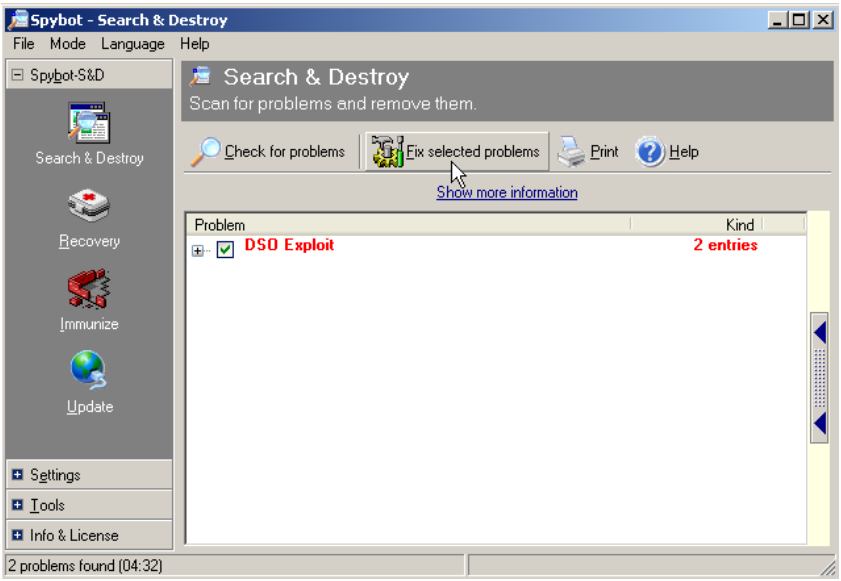


As with AdAware, you can either click on every update, or right-click with the mouse cursor in the window where shown, and choose *Select All,* then click the *Download Updates* button.

Either if you haven't scheduled it to run automatically, or you just received a set of updates, or it just hasn't been run for a while, click on *Search & Destroy* (the top-left button), then click on *Check for Problems*.



Again, this will take a few minutes to run. Watch the bottom of the *Spybot* window for a progress indicator. You hope it won't find anything; if it does, it'll look something like this:



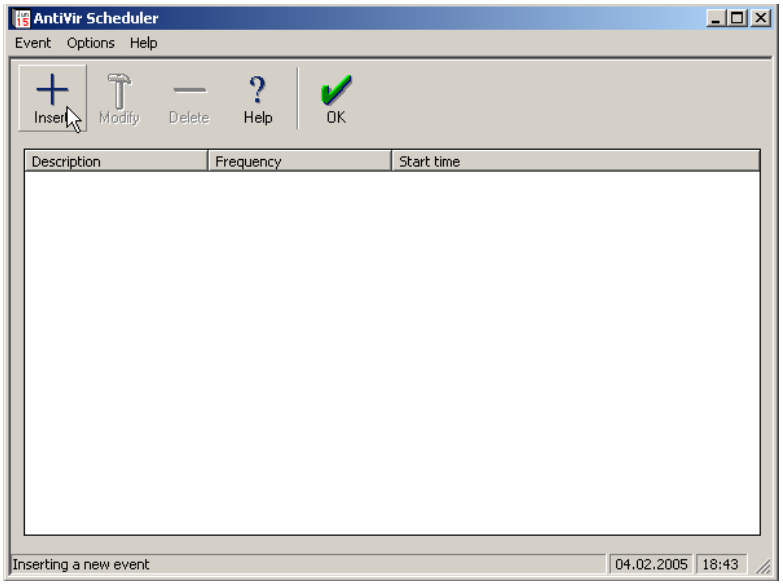
Click on *Fix selected problems*. It will tell you how many will be removed, and then do so. It will then pop up a dialog box telling you it removed problems; click OK. Sometimes, it may find that it can't remove a problem without rebooting and letting itself run as the first program started by Windows; it's worth doing this, so allow it to do so. Otherwise, just exit the program.

Now to warn you about a problem with the "Tea-Timer". This module watches for anything trying to insert or change your system configuration. However, the author identified a problem with the development kit from the company he was using; when reported, he was ignored. SO, he decided to leave the bug visible in his software as a protest. This makes responding to Tea-Timer warnings a bit difficult, since the bug manifests as overlaying one message right on top of the button you need to use to respond to the warning! Simply enough, use careful mouse positioning to select the "Accept" button on the left or "Deny" on the right. You can also use the "A" button to Accept, if the warning dialog box is highlighted.

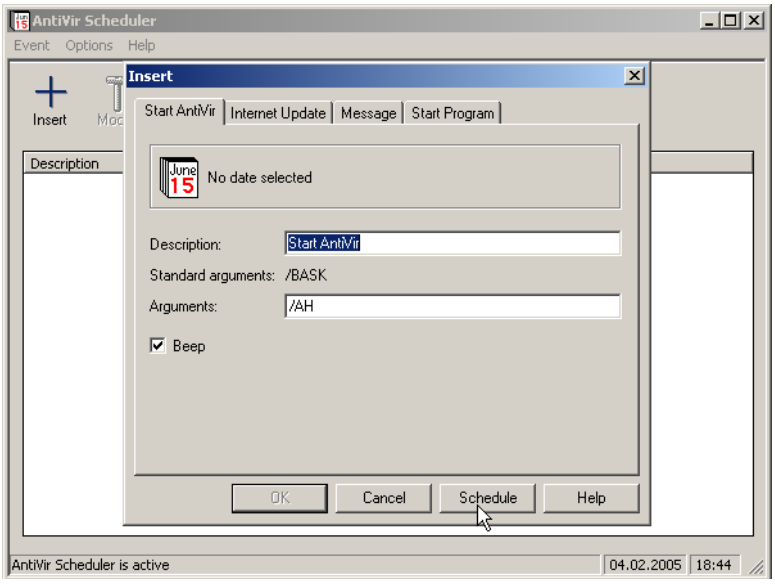
6.4 ANTI-VIRUS

Of course, if you have another anti-virus program, none of this will apply to you, but the concept is the same—get it to (a) go out and update itself automatically, and (b) scan the system automatically. These instructions are specifically for scheduling AntiVir.

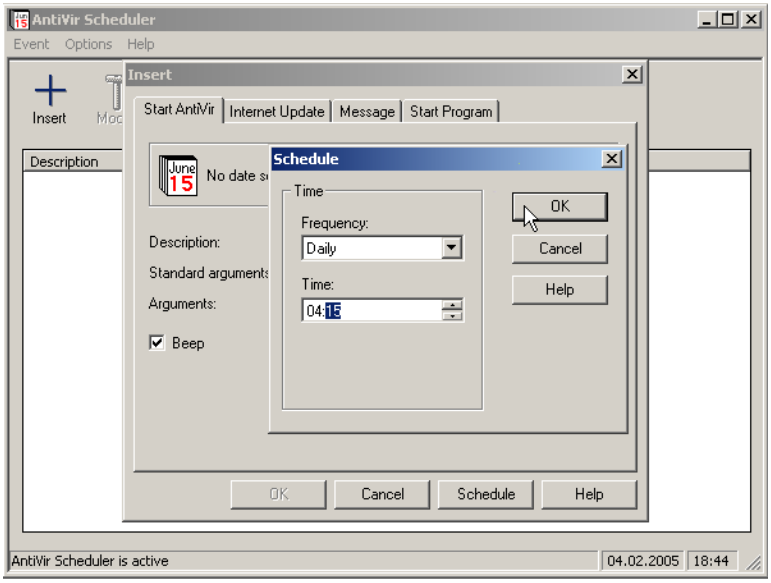
AntiVir will automatically update and scan, *if* you schedule these activities. Run the *AntiVir Scheduler* from *Start->Programs->Antivir Personal Edition->Antivir Scheduler*. Click on *Insert*.



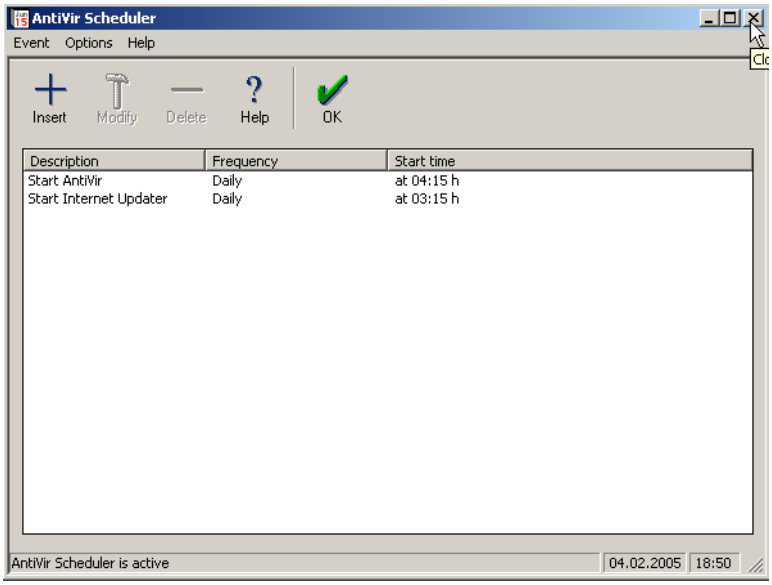
When you click *Insert*, you'll see four tabs—two are the ones we want, *Start AntiVir* and *Internet Update*. We'll start scheduling the AntiVir scan itself. Let's assume your computer is always on, and can scan at 4:15 in the morning every day. Click on the *Schedule* button of the *Start AntiVir* tab:



After you've selected the day to run (we picked every day) and time, the screen will look like this:



Click OK, then click on the *Internet Update* tab and set the schedule the same way; let's assume you allow an update check every day at 3:15 in the morning. When done with that, click the *OK* button on the *Insert* dialog box. Your schedule screen should look like this when done:



Go ahead and close the scheduler; you're done. AntiVir will scan and update automatically.

6.5 BACKUP

Since it's buried so deeply (*Start->Programs->Accessories->System Tools->Backup*), you probably want to create a shortcut on your desktop for this program. To do this, while the cursor is over the *Backup* program menu choice, click and hold down the right mouse button, and drag

the item to the Desktop and let go. It will ask if you want to create a shortcut (or it may ask to copy); select either choice, but *don't* select to "move" it!

The simplest approach is to use the *Backup Wizard* that is offered when you start Backup. As you go through the interview to create your backup job, remember, in order, to select:

- ✓ Backup selected files, drives, or network data.
- ✓ Open "My Computer" and back up whatever will fit on your destination backup media. If it's a big, removable hard drive, select all of your hard drives (except, of course, that drive.) If it's just a directory on another drive in your computer, or some other, smaller, storage, pick and choose—generally, just your own files (memos, Quicken files, etc.)
- ✓ Select the backup media name. Make it something that will make sense to you—e.g., "050204_Fullback.bkf" for a full system backup made on Feb. 4, 2005. (Why put it YYMMDD? Because this sorts in a directory listing from oldest to newest!)
- ✓ When you get to the "Completing the Backup Wizard" screen, you are *not* done! Click the *Advanced* button.
- ✓ Accept a "Normal" backup in the next screen.
- ✓ Click on "Verify data after backup" on the following screen.
- ✓ Click on "Replace the data on the media with this backup" on the next screen.
- ✓ Just accept the labels that Backup offers in the next screen.
- ✓ Change the backup to *Later* in the *When to Back Up* screen. If you're running Windows 2000 or XP, it'll probably ask for your login and password, because when it *does* run the job, it needs to log in. Give it to the program, unless you're not a privileged user; then give it the Administrator login and password.
- ✓ Give the job some meaningful name, such as "Fullback". Click on "Set Schedule", and schedule the job for whenever you want it to run.
- ✓ Finish.

You can guess—this is much more complicated, with a lot more choices, than just doing a system anti-virus scan. If you need to, ask a tech friend to help out!

7. CONCLUSION

This paper has attempted to describe, from theory to practice, what kind of malware exists, what it can do, and how to protect your system from it. It is, necessarily, only a start; there is a wealth of more in-depth information on the Internet. Good luck, and good hunting!