

Desktop Guerrillas

GUERRILLA BRIEFS

In the past few years, a new breed of programs has invaded desktops. Usually termed “spyware” or “adware,” these products have various goals, from displaying annoying ads to capturing passwords and credit card numbers. Occurrence of these programs has reached epidemic levels; in a recent study by the National Cyber Security Alliance, 91% of computers surveyed were infested with spyware.

HOW DO I KNOW IF I'M INFECTED?

One of the best ways of detecting these applications is to run a scanner designed to detect them. But even without a scanner, symptoms are usually easy to spot.

- Pop-up ads appear when not browsing sites.
- Internet Explorer's home (default) page has changed.
- Extra buttons or “search bars” appear on your screen.
- Sluggish performance is evident.
- Complete loss of network connectivity occurs.

HOW DID THIS HAPPEN IN THE FIRST PLACE?

There are a number of ways that you can become infected.

Installing the wrong program. One of the most common ways of getting spyware is to install programs that you don't realize contain malicious components. These programs often come disguised as helpful products, such as a search bar, a utility to dress up your email, or even, ironically, a spyware protection program.

Visiting the wrong site. A website may take advantage of a flaw in Internet Explorer and trigger installation of a program, even without your consent.

Opening the wrong email. Spammers may send you to a link that triggers an install. Don't be fooled by emails that look like they're from trusted parties—PayPal, eBay, a bank—it's very easy to make a letter look genuine even when it's not. These emails may ask for confidential information or trigger an install of their malicious code.

WHY ME?

Where virus writers are often out for glory among their peers, spyware authors have a less noble goal: the almighty dollar. By installing their software on your system, they hope to make a fraction of a penny when you click on their ads. These numbers quickly add up and provide a tidy sum for the authors.

REMOVAL

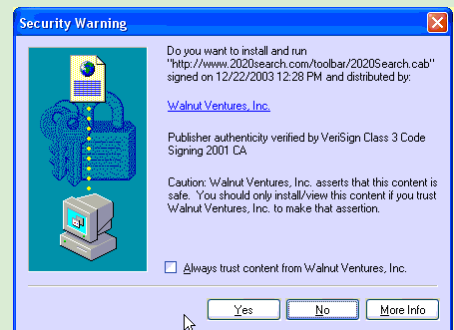
Here's the (really) bad news. If you have a moderate to severe infection, you're much better off either enlisting a professional or rebuilding your computer from scratch. Unlike virus protection, where any of the popular antivirus products will provide adequate defense, the sheer number of spyware developers, and the especially insidious nature of how the spyware invades computers, makes it impossible for any one program to detect and remove them all.

Our removal process always goes beyond running anti-spyware tools; we also comb

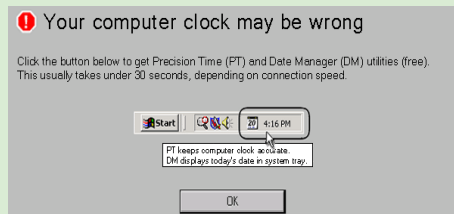
KNOW THINE ENEMY

Keeping your computer free of malicious programs is harder than ever. Here are some tips to protect yourself.

ROGUES GALLERY



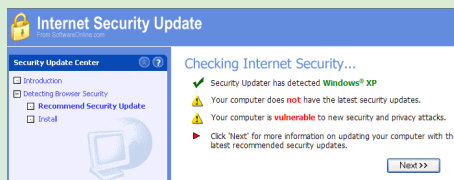
These security prompts are asking to install new software onto your system. Do not answer “yes” unless you know what is being installed!



Many spyware programs come in the guise of needed applications. This one promises to keep your time synchronized. Not only is this unnecessary - Windows XP does this for you - but installing this application brings many other ones with it.



Some windows look like messages from your operating system. It takes a little experience to separate the real messages from the fake ones, but the word “advertisement” in title bar should instantly raise suspicions.



Popups sometimes make themselves look like trusted applications (such as Windows Update). Examine these closely and close them if they appear suspicious.

through startup items, Internet Explorer components, and network protocols manually to investigate and remove anything suspicious. If you do decide to use some of our recommended applications to clean up your system, be absolutely sure that you not only have your important files and email backed up, but you also have recovery CDs at the ready.

PROTECTION

Don't go back to your Underwood just yet. While there's no silver bullet for eliminating the threat of spyware, there are a few simple precautions that you can take to reduce your risk.

Set your system to automatically check for and apply critical updates.

As we've said before, just visiting the wrong website can expose your computer to the installation of spyware. Malicious parties do this by finding and exploiting bugs in Microsoft Windows. As Microsoft discovers these bugs, they release patches for users to download and install. You can download these patches manually by visiting the "Windows Update" site, or configuring your computer for automatic updates.

Not to be ignored are the Microsoft Office updates, as those improve security as well. Visit www.microsoft.com/office and follow the links to "Office Update." Unfortunately, there is no provision here for automatic updates, but you should make an effort to visit that site monthly to check for patches.

Just say no.

If you visit an unfamiliar website, and are presented with a popup inviting you to install a product, be sure to click "no," or even better, click on the X in the upper right hand corner of the window. This is the safest way of avoiding accidental installation of these products. Also, keep an eye on those who "just want to check their email" on your computer. A well intentioned coworker could easily install something undesirable.

Keep the kids away from the computer.

A study by Symantec found that most spyware creators target children in order to install their products. Spyware is inevitable when kids are involved. As such, provide them with alternatives to using your office system. New computers can be found for under \$500 today. Keep the reinstallation media handy so that you can restore the computer to pristine shape as necessary.

Update your antivirus.

Make sure your antivirus software is not only active, but the subscription is current. Although viruses and spyware are two different products, many antivirus products are improving in their ability to catch spyware. For this purpose, a lesser known product, NOD32, is one of the most effective.

IT'S A THIN LINE

Nowadays, it's not always clear what is spyware and what isn't. Programs like WeatherBug, installed by AOL Instant Messenger, are popular on office computers, and are fairly well behaved, but that doesn't mean they don't impact your computer's performance. Be cautious about the products you install on your system, and your computer will lead the long and happy life it deserves.

Desktop Guerrillas is an IT consulting firm serving small businesses in Fairfield County. We'll not only remove spyware from your infested systems, but we'll help implement security policies that will keep them at bay.

USEFUL TOOLS AND SITES

Ad-Aware

Ad-Aware is one of the oldest and most respected of the spyware applications. Their personal version, free for home use, is an effective scanning and removal tool.

<http://www.lavasoft.com/>

Spybot Search & Destroy

Spybot is another product, free for both home and business use. Their product is a little less intuitive than the other programs, but it does offer some real time protection against spyware even running.

<http://www.safer-networking.org/>

Microsoft Antispyware

Microsoft went out and purchased one of the leading antispyware products, and now offers it for free. It's an excellent product,

but is somewhat resource-hungry; on slower computers you may want to uninstall after a cleanup.

<http://www.microsoft.com/>

HijackThis

HijackThis gives you the ability to examine and disable startup items, as well as "browser helper objects" – applications that interface with your Internet browser and . HijackThis is an advanced tool, with web sites dedicated to interpreting its output. Recommended for experts only.

<http://www.tomcoyote.org/hjt/>

Be sure to download these applications – or any other applications you might choose – from the original developers, as spyware developers have been known to repackage these programs with spyware built into them.