

How Does Spyware, Malware or Crapware Get on My Computer?

Have you ever wondered how malware, spyware, scareware, crapware, or other undesirable software might get on a computer? First we'll illustrate how easily your system can be infected, and then we'll show you how to clean it up.

Our example system, running Windows 7, was set up from a worst case scenario point of view: Someone who was only interested in quickly getting to all the "fun stuff" on the internet with absolutely no concern for personal or computer security.

Freshly Installed – Pre Malware

Here you can see the number of processes (and type) that were running on our freshly installed Windows 7 system. The install was so fresh that the only protection that this system had was the Windows Firewall and Windows Defender to keep the malware and virus hordes at bay.

The screenshot shows the Windows Task Manager interface with the 'Processes' tab selected. The list of processes is as follows:

Process Name	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	70.87		
Interrupts	n/a	3.92	Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	256		Windows Session Manager	Microsoft Corporation
csrss.exe	332		Client Server Runtime Process	Microsoft Corporation
wininit.exe	380		Windows Start-Up Application	Microsoft Corporation
services.exe	468		Services and Controller app	Microsoft Corporation
svchost.exe	604		Host Process for Windows Services	Microsoft Corporation
WmiPrvSE.exe	2604		WMI Provider Host	Microsoft Corporation
svchost.exe	668		Host Process for Windows Services	Microsoft Corporation
svchost.exe	772		Host Process for Windows Services	Microsoft Corporation
svchost.exe	824	22.33	Host Process for Windows Services	Microsoft Corporation
dwm.exe	1540		Desktop Window Manager	Microsoft Corporation
svchost.exe	852		Host Process for Windows Services	Microsoft Corporation
svchost.exe	968		Host Process for Windows Services	Microsoft Corporation
svchost.exe	1048		Host Process for Windows Services	Microsoft Corporation
spoolsv.exe	1196		Spooler SubSystem App	Microsoft Corporation
svchost.exe	1228		Host Process for Windows Services	Microsoft Corporation
svchost.exe	1360		Host Process for Windows Services	Microsoft Corporation
taskhost.exe	1408		Host Process for Windows Tasks	Microsoft Corporation
SearchIndexer.exe	624		Microsoft Windows Search Indexer	Microsoft Corporation
SearchProtocolH...	3072		Microsoft Windows Search Protocol Host	Microsoft Corporation
sppsvc.exe	1800		Microsoft Software Protection Platform Service	Microsoft Corporation
svchost.exe	1576		Host Process for Windows Services	Microsoft Corporation
lsass.exe	484		Local Security Authority Process	Microsoft Corporation
lsmd.exe	492		Local Session Manager Service	Microsoft Corporation
csrss.exe	392		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	432		Windows Logon Application	Microsoft Corporation
explorer.exe	1564		Windows Explorer	Microsoft Corporation
procexp.exe	2924	1.94	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com

At the bottom of the window, system statistics are displayed: CPU Usage: 29.13%, Commit Charge: 18.16%, Processes: 29, Physical Usage: 31.20%.

How Some Malware Gets On Your Computer

Malware, spyware, and other junk software makes it onto your computer for a number of reasons:

- You installed something you really shouldn't have, from an untrustworthy source. Often these include screensavers, toolbars, or torrents that you didn't scan for viruses.
- You didn't pay attention when installing a "reputable" application that bundles "optional" crapware.
- You've already managed to get yourself infected, and the malware installs even more malware.
- You aren't using a quality Anti-Virus or Anti-Spyware application.

Watch Out for Insidious Bundled Crapware

One of the biggest problems recently is that the makers of popular software keep selling out, and including "optional" crapware that nobody needs or wants. This way they profit off the unsuspecting users that aren't tech-savvy enough to know any better.

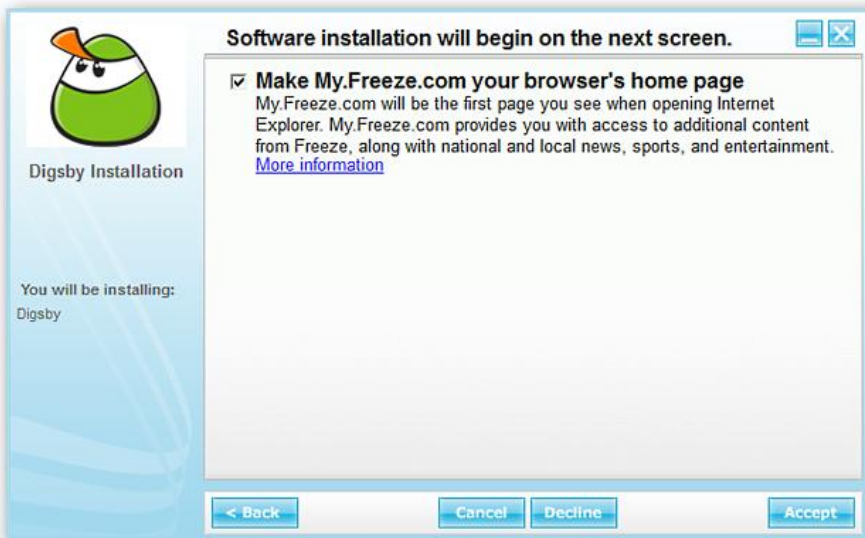
On our example system we installed Digsby Messenger, a very popular "reputable" application. This was the regular install version and as you can see in the following screenshots, there are attempts to get you to install undesirable software or make "not so good" changes on your computer. If a person is not careful, then their system becomes infected.

Here you can see the attempt to add the "My.Freeze.com Toolbar" to your browser(s)...definitely not good! Notice that while it does state that the software may be removed later, some people may 1.) Not notice it (lack of attention), 2.) Be in too much of a hurry to install the software to notice, or 3.) Not be familiar or comfortable with removing the software after it is already installed on their system.

The real trick with Digsby (and other software that is set up with the same installation style) is that clicking on "Decline" still allows the installation of Digsby itself to proceed. But can you imagine how things can end up for those people who may think or believe that the only way to get Digsby or similar software installed is to click on "Accept"? It has a really deceptive style!



A very obvious attempt to make “My.Freeze.com” the new homepage for your browser(s). Once again the “Decline” versus “Accept” dilemma combined with a checkmark selection choice...



If you have many programs that attempt to install “value-added” software like this on your system, you will quickly find that the majority (or all) of your operating system’s resources are being used up by malware (i.e. background processes). You are also likely to find that you will have unstable or very sluggish browser response, and are likely to have your personal and computer’s security compromised.

Just How Quickly Can a System Become Infected?

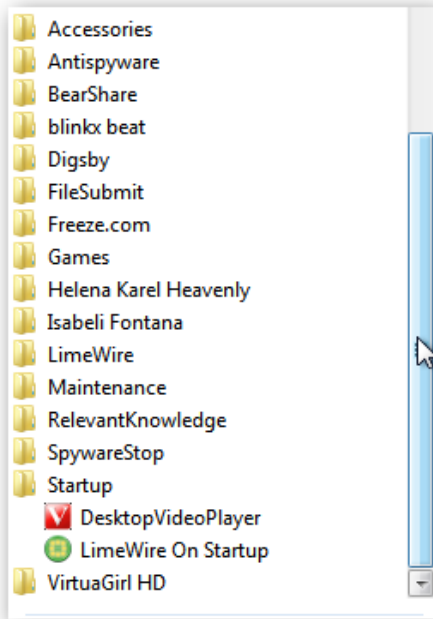
It only took 2.5 hours to reach the level described in our article... simply surfing wherever for “whatever looked interesting or different”, downloading things like screensavers, file-sharing applications, and installing questionable software from advertisements.

The possibilities for becoming infected with viruses or malware were rather high with little to no protection or forethought given concerning what was installed or for the websites visited. Searches for various “less than desirable” pictures, screensavers, clicking on ads, etc. made it very easy to find trouble... perhaps the better way to phrase that is that it was very easy for trouble to find our example system.

Here you can see a screenshot of the desktop of our example system. Notice that there are icons for file sharing programs, fake anti-malware programs, icons for various screensavers, less than nice websites (possible additional infection vectors), and a virtual dancing woman. Nothing good here!



Here is a look at the Start Menu... notice that some of the malware has obvious shortcuts in the Startup Folder, but there were plenty on our example system that were not shown in this folder.

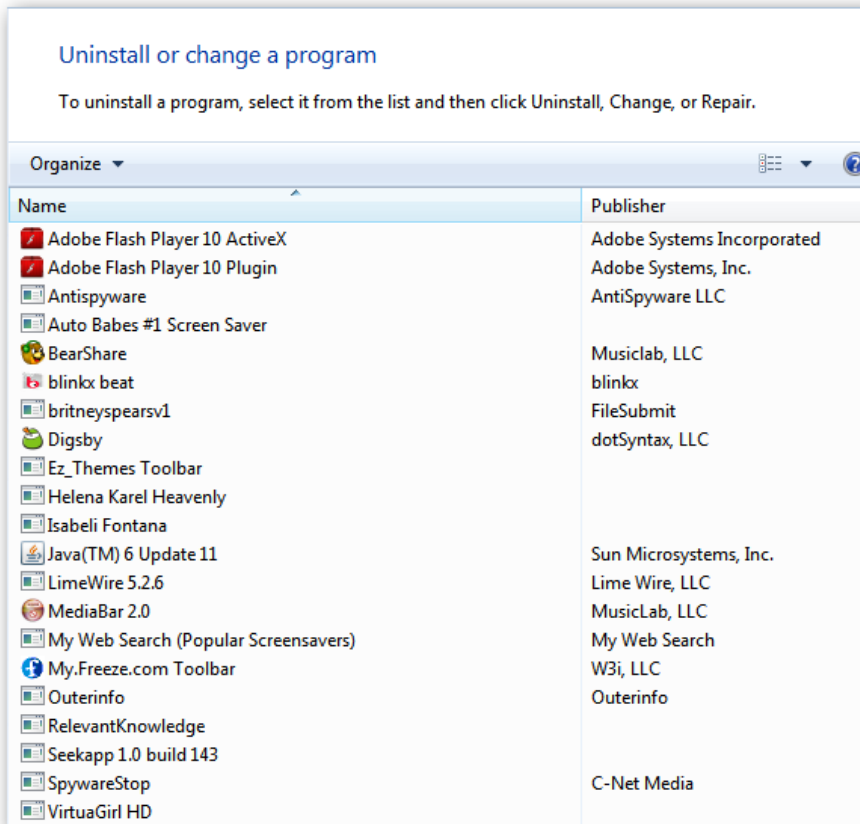


A quick look at an over abundance of toolbars plaguing Internet Explorer 8...by this point the browser was already having some problems starting properly (very slow), some episodes of crashing, and some browser hijacking had occurred.



Taking a peek at the Program Uninstall Window shows a variety of malware and undesirable software types that were on our example system.

Note: These are the ones that actually bothered with listing an entry in the Uninstall Registry.



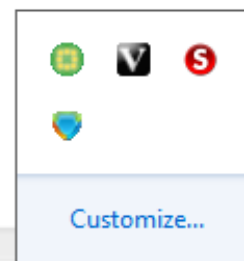
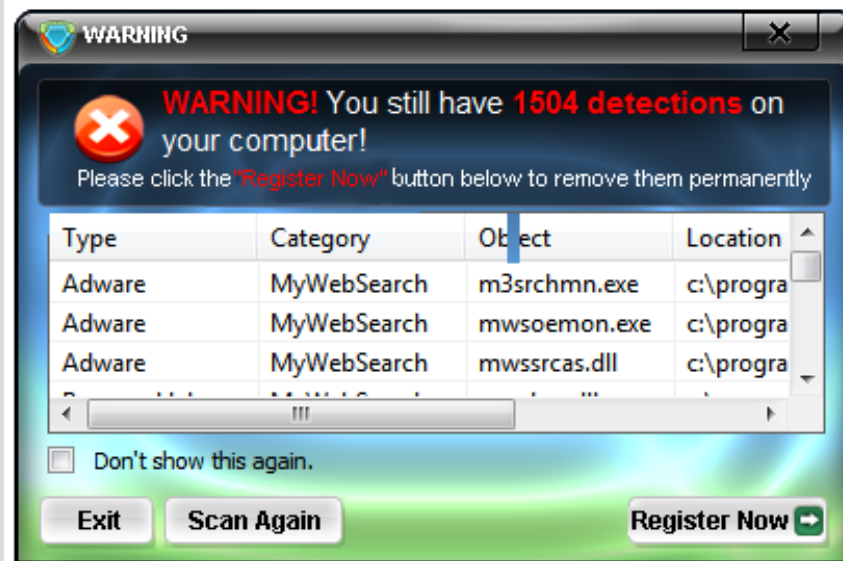
A Good Look at Scareware

What is scareware? It is software that once installed on your system will try to trick you into believing that you have a highly infected system with some very high “numbers of infections” found. These programs will constantly bother you to register and purchase the software in order to clean up your computer system.

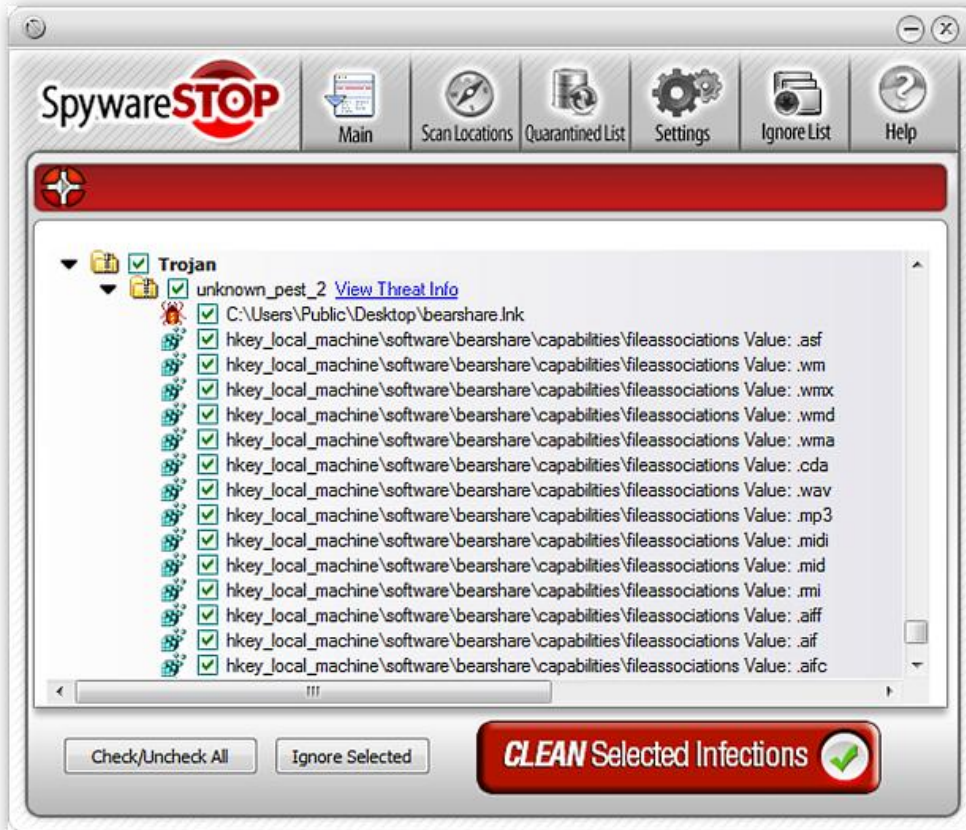
Here you can see two examples of well known scareware. SpywareStop and AntiSpyware 2009. Do not be surprised if you notice that these two “separate” softwares seem to be extremely alike in looks, style, and operation. They are exactly alike...the same wolf just different sheep skins. This is a common practice to stay ahead of legitimate anti-malware and anti-virus software and not be deleted before hopefully being purchased by unsuspecting computer users.

A good look at the two screens that appeared every time we started our example system...absolutely no hesitation to “remind us” how infected our computer was and that we should register the software now. Disgusting!!

Note: The SpywareStop website was presented to us courtesy of a browser hijacking...and of course we were encouraged to install it.



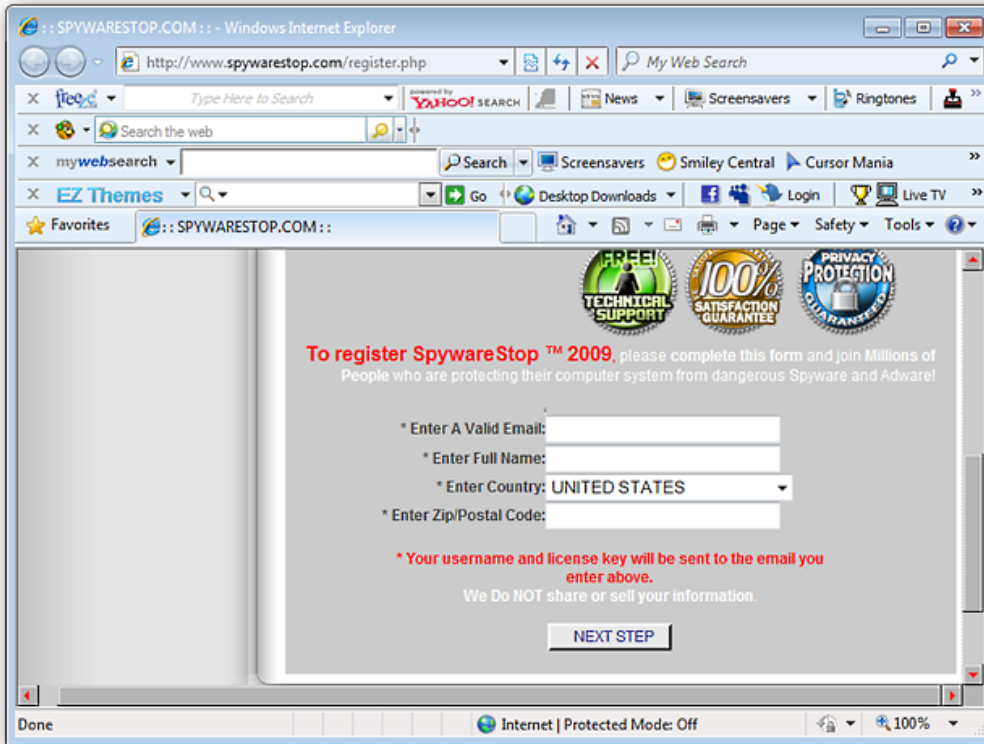
The main window for SpywareStop...oh so quick to try and encourage you to remove the infections.



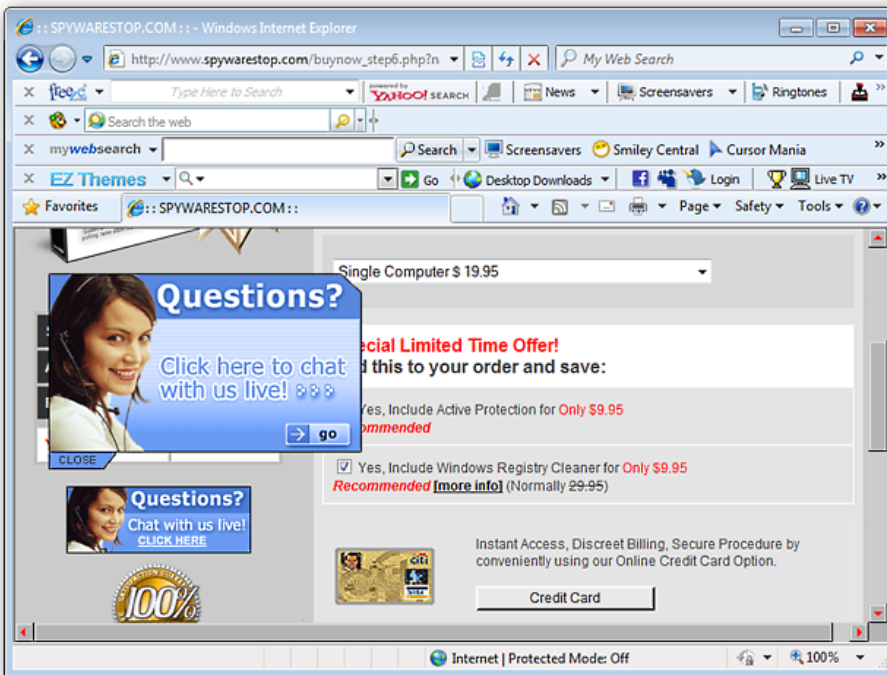
The System Tray pop up window for SpywareStop...



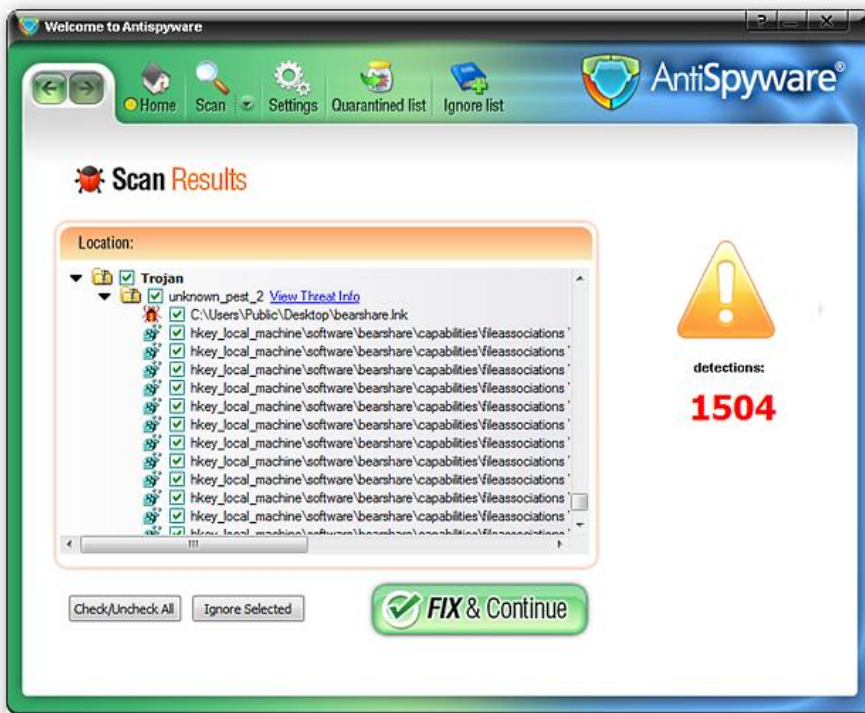
What do things look like if someone went to register the software and purchase it? The registration starts with a request for basic information including an e-mail address. Chances are the addresses harvested in this manner will be sold to spammers...the potential for a little extra income will definitely have an appeal.



Notice that additional services and software are readily available! Nothing like an opportunity to make even more easy money once they have someone this far in...and of course you can use your credit card. How convenient for them...



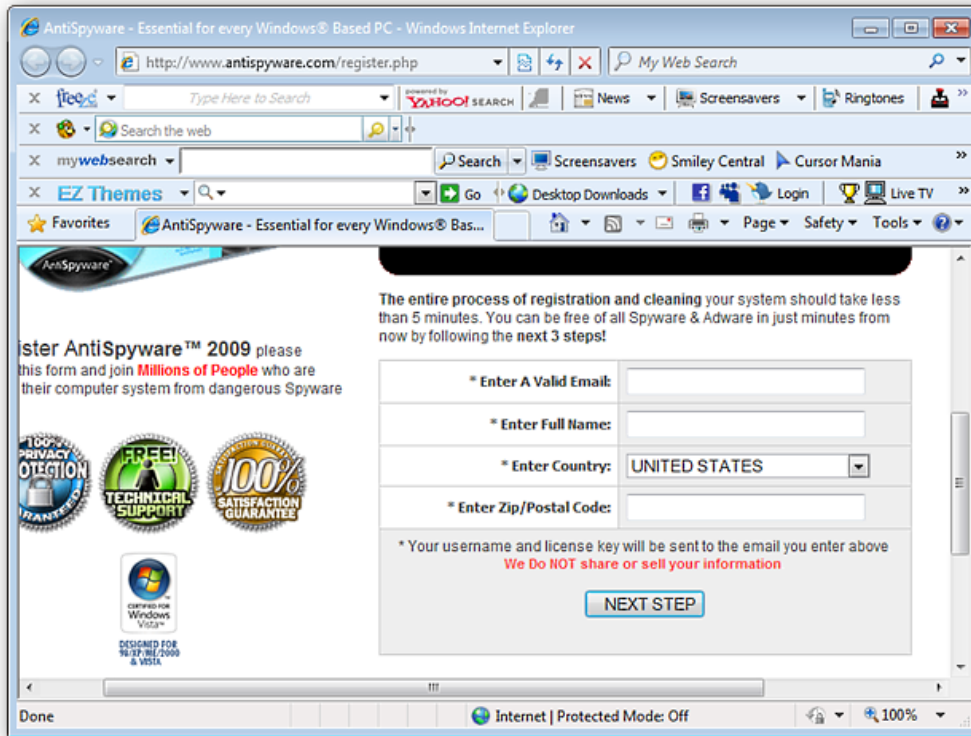
The ever wonderful cousin to SpywareStop...the infamous AntiSpyware 2009 (also very well known with the 2008 designation).



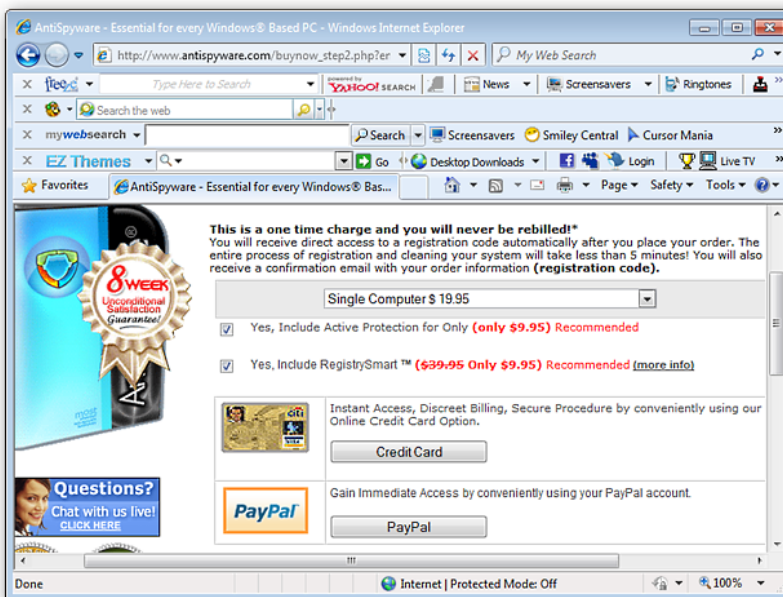
And the wonderful System Tray pop up window for AntiSpyware 2009...the fun never stops!



What about registration for this one? Take a good look at these two screenshots and compare them with the two shown above. There is so little difference...yet another sign that these are identical scareware programs with altered user interfaces and alternate websites.

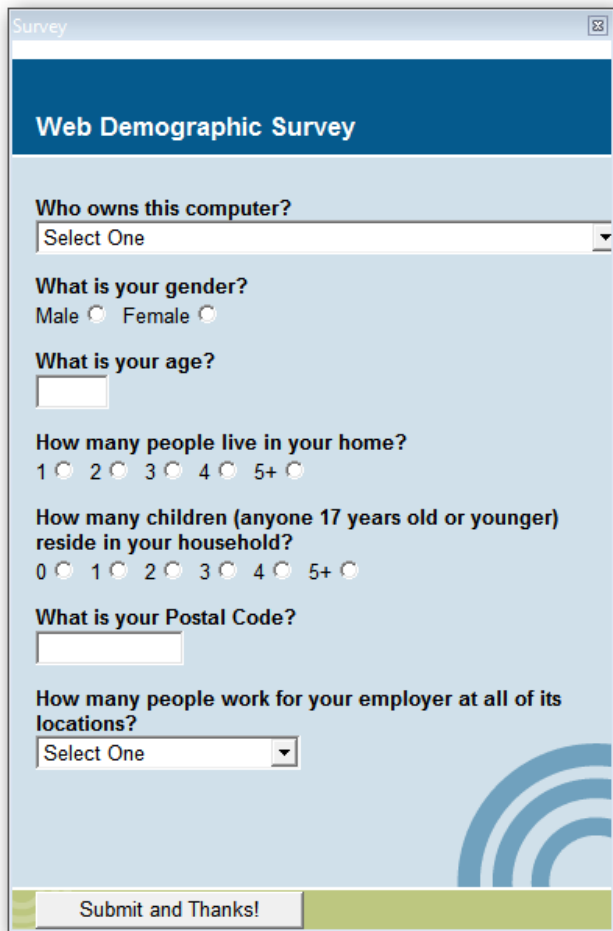


How nice! More additional software available for you to buy and the ability to use that credit card and PayPal!



Some Other Things That Come with Malware

Here is another irritating feature of some malware. Nice pop up windows harassing you to take surveys or do other things. This was an additional “gift” from one of the programs installed on our example system.



The image shows a screenshot of a web browser window titled "Survey". The main heading is "Web Demographic Survey". The survey contains the following questions and input fields:

- Who owns this computer?** (Dropdown menu with "Select One" selected)
- What is your gender?** (Radio buttons for Male and Female)
- What is your age?** (Text input field)
- How many people live in your home?** (Radio buttons for 1, 2, 3, 4, 5+)
- How many children (anyone 17 years old or younger) reside in your household?** (Radio buttons for 0, 1, 2, 3, 4, 5+)
- What is your Postal Code?** (Text input field)
- How many people work for your employer at all of its locations?** (Dropdown menu with "Select One" selected)

At the bottom of the window is a button labeled "Submit and Thanks!".

A Look at the Processes Running After Infection

Compare the screenshot of running processes shown at the beginning of the article and then the running processes shown here. You can already see a significant increase. Not good for you or your computer!

System Idle Process	0	90.41		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	0.93		
smss.exe	252		Windows Session Manager	Microsoft Corporation
csrss.exe	328		Client Server Runtime Process	Microsoft Corporation
wininit.exe	376		Windows Start-Up Application	Microsoft Corporation
services.exe	456	1.86	Services and Controller app	Microsoft Corporation
svchost.exe	592		Host Process for Windows Services	Microsoft Corporation
WmiPrvSE.exe	2680		WMI Provider Host	Microsoft Corporation
unsecapp.exe	2888		Sink to receive asynchronous callbacks for WMI client applicati...	Microsoft Corporation
svchost.exe	656		Host Process for Windows Services	Microsoft Corporation
svchost.exe	704		Host Process for Windows Services	Microsoft Corporation
svchost.exe	828		Host Process for Windows Services	Microsoft Corporation
dwm.exe	1220		Desktop Window Manager	Microsoft Corporation
svchost.exe	868		Host Process for Windows Services	Microsoft Corporation
taskeng.exe	1708		Task Scheduler Engine	Microsoft Corporation
svchost.exe	976		Host Process for Windows Services	Microsoft Corporation
svchost.exe	1080		Host Process for Windows Services	Microsoft Corporation
spoolsv.exe	1356		Spooler SubSystem App	Microsoft Corporation
svchost.exe	1564		Host Process for Windows Services	Microsoft Corporation
taskhost.exe	1576		Host Process for Windows Tasks	Microsoft Corporation
svchost.exe	1876		Host Process for Windows Services	Microsoft Corporation
MWSSVC.EXE	1936		My Web Search Bar	MyWebSearch.com
rlservice.exe	1988		RelevantKnowledge	TMRG, Inc.
rlvknlg.exe	4076		RelevantKnowledge	TMRG, Inc.
seekapp143.exe	2020			
seekappsrch.exe	348			
SearchIndexer.exe	1108		Microsoft Windows Search Indexer	Microsoft Corporation
svchost.exe	2200		Host Process for Windows Services	Microsoft Corporation
spsvc.exe	3604		Microsoft Software Protection Platform Service	Microsoft Corporation
svchost.exe	3788		Host Process for Windows Services	Microsoft Corporation
lsass.exe	464		Local Security Authority Process	Microsoft Corporation
lsmd.exe	472		Local Session Manager Service	Microsoft Corporation
csrss.exe	388		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	428		Windows Logon Application	Microsoft Corporation
explorer.exe	1244		Windows Explorer	Microsoft Corporation
jusched.exe	1364		Java(TM) Platform SE binary	Sun Microsystems, Inc.
M3SRCHMN.EXE	1380		MyWebSearch SearchScope Monitor	MyWebSearch.com
MWSEMON.EXE	1388		My Web Search Plugin Loader	MyWebSearch.com
blinkx.exe	1396		Blinkx	Blinkx Limited
vghd.exe	1412		VirtuaGirl HD main executable	Totem Entertainment
VirtuaGirl_Downloa...	1540		VirtuaGirl HD Download Manager	Totem Entertainment
LimeWire.exe	1420	0.93	LimeWire	Lime Wire, LLC
notepad.exe	2908		Notepad	Microsoft Corporation
procexp.exe	2816	5.59	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com

CPU Usage: 9.32% Commit Charge: 30.29% Processes: 44 Physical Usage: 50.90%

Conclusion

While nothing super horrible got onto our example system within those 2.5 hours, it is still easy to see just how quickly a system can start to become a mess. Imagine a system that has been exposed for a much longer period of time and is heavily infected! The best approach is to avoid trouble from the beginning. But if you find yourself or someone you know with an infected system then take a look at our upcoming series on removing malware from an infected computer.