Virus/Spy-Ware Protection

Introduction

Viruses and the subset of viruses called Spy-ware or Ad-ware, are one of the biggest problems facing modern computers; and probably cause more anxiety than any other computer related topic. A virus is any file that intentionally negatively impacts a computer's performance; usually these are entered onto a computer without the user's knowledge. Spy-ware and Ad-ware are similar in their method of transfer onto a computer, for this reason they are frequently lumped together, but they differ in their purpose. Spy-ware is a general term for programs that, when running on a computer, monitor web histories and other information passed over the internet. Ad-ware consists of programs that cause advertising banners and pop-up windows to appear while you use the Internet. These types of programs pose a major threat to all computers currently working with the Internet. Today's class will discuss viruses, specifically those two kinds of viruses, and what can be done to minimize the user's risk.

Viruses

What are they?

"A virus is a parasitic program written intentionally to enter a computer without the user's permission or knowledge. The word parasitic is used

because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some viruses do little but replicate, others can cause serious damage or affect program and system performance. A virus should never be assumed harmless and left on a system." -- Symantec

How do I know if I have a virus?

http://www.ucs.ed.ac.uk/usd/iss/ol/issues/viruses/howdo.html

Protective Software (Stopping problems before they start)

1. Third party software: Programs like Norton or McAfee antivirus are designed to run in the background of you computer use. Meaning that they will constantly be on no matter what else the computer is doing and will only appear when a problem arises. These programs provide protection from known viruses but to remain relevant they need to be periodically updated with all of the new virus definitions available. This is usually not free and even with these measures in place it isn't guaranteed that a computer is safe (although it does help a lot). If you have one of these programs it will periodically notify you that new virus definitions are available and then, if you are paying them, the definitions will download and self-install.

2. Built in protection (ISP/Email): Most Email services will scan downloads before approving their being saved to a computer. This can help

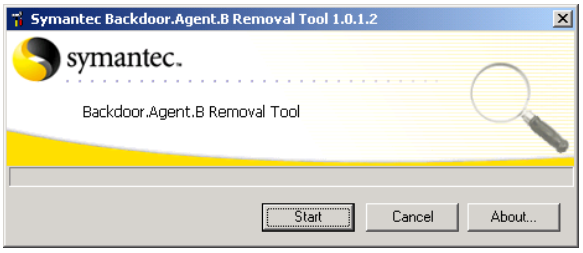
to warn you about very straightforward and destructive viruses but it's far from foolproof.

Dealing with Virus Problems (Fixing what they break)

Most of the techniques we'd used to fix virus damage will be discussed in more detail later on (in the Spy-ware section) but for right now I want to go over the main way to repair virus damage.

-Download a virus specific patch:

1. Go to anti-virus companies web page (http://norton.com/ for today's example)
2. Download virus removal (selecting the virus you are having problems with or just trying lots of them)
3. Save the tool to the computer's desktop
4. Double-click on the file now on computer's desktop to start the program



5. Left-click the "Start" button
6. Program should complete the task itself, follow any prompts and restart when indicated

Spy-Ware/Ad-Ware

What is it and where does it come from?

-Adware, also known as an Adbot, can do a number of things from profile your online surfing and spending habits to popping up annoying ad windows as you surf. In some cases Adware has been bundled (i.e. peer-to-peer file swapping products) with other software without the user's knowledge or slipped in the fine print of a EULA (End User License Agreement).

Not all Adware is bad, but often users are annoyed by adware's intrusive behavior. Keep in mind that by removing Adware sometimes the program it came bundled with for free may stop functioning. Some Adware, dubbed a "BackDoor Santa" may not perform any activity other then to profile a user's surfing activity for study.

AdWare can be obnoxious in that it performs "drive-by downloads". Drive-by downloads are accomplished by providing a misleading dialogue box or other methods of stealth installation. Many times users have no idea they have installed the application. Often Adware makers make their application difficult to uninstall.

A "EULA" or End User License Agreement is the agreement you accept when you click "OK" or "Continue" when you are installing software. Many users never bother to read the EULA.

It is imperative to actually read this agreement before you install any software. No matter how tedious the EULA, you should be able to find out the intent BEFORE you install the software. If you have questions about the EULA- e-mail the company and ask them for clarification. If they cannot clarify this do not install the software.

-Spy-ware is potentially far more dangerous threat than Ad-ware because it can record your keystrokes, history, passwords, and other confidential and private information.

Spy-ware is often sold as a spouse monitor, child monitor, a surveillance tool or simply as a tool to spy on users to gain unauthorized access.

Spy-ware is also known as: snoop-ware, PC surveillance, key logger, system recorders, Parental control software, PC recorder, Detective software and Internet monitoring software.

Spy-ware covertly gathers user information and activity without the user's knowledge. Spy software can record your keystrokes as you type them, passwords, and credit card numbers, sensitive information, where you surf, chat logs, and can even take random screenshots of your activity. Basically whatever you do on the computer is completely viewable by the spy. You do not have to be connected to the Internet to be spied upon.

The latest permutations of Spy-ware include the use of routines to mail out

user activity via e-mail or posting information to the web where the spy can view it at their leisure. Also many spy-ware vendors use “stealth routines” and “polymorphic” (meaning to change) techniques to avoid detection and removal by popular anti-spy software. In some cases spyware, known as a retrospy, will counter-attack anti-spy packages by attempting to disable the program. In addition they may use routines to re-install the spyware application after it has been detected.

<<For efficiencies sake I will only type “Spy-ware” for the rest of the instructions but the reader can assume that I mean “Spy-ware” and “Ad-ware”>>

Protecting Your Computer

1. Internet Options: Increasing the security settings on Internet Explorer and reducing the acceptance of cookies can limit the amount of Spy-ware transmitted to a computer. However, this also limits the amount of places a user can effectively visit and the resources a user can take advantage of. This is the balance between safety and effectiveness that must be kept in mind when securing a computer.

2. Third party programs: Many of the same programs that will be discussed in detail in the “repairing” section of our talk about Spy-Ware can be used to prevent damage as well. These programs work like a filter, preventing

damaging files from getting through and notifying the user of anything that might be a problem. This is good because it stops the Spy-Ware damage before it starts. Unfortunately, there are disadvantages, the user often has to pay for these services (while the sweep is free); the filter doesn't necessarily catch everything; and it will catch things that aren't damaging.

3. Freezing: There are products available that will effectively "Freeze" your hard drive – preventing any changes whatsoever from being made. As you use the computer things will operate as normal, but when it is restarted any changes that were made will be restored back to the frozen state. This is an effective way of preventing Spy-Ware problems but can make it inconvenient to use the computer (it has to be unfrozen before any change is made, which requires a restart, and then frozen again after the change is made, which requires another restart). A "thawed" space, where changes are possible, can be created but that makes a fairly technical setup even more complicated.

<u>Repairing the Damage</u>

Some techniques specific to Spy-ware/Ad-ware that should be considered *IN ADDITION* to those introduced during the Virus section of the class.

1. Third party programs: There are a number of programs designed to "sweep" or search through the contents of your computer to try to find

anything that might be Spy-ware or Ad-ware related. Some of these are free, others will give you some services for free but cost more for expanded features, still others you need to buy outright. The programs are consistent in how they operate; first they perform a search through the computers contents, then they report suspect files to the user, then the user selects the files that he wants removed, finally the program quarantines and deletes the suspected files.

-Pros: Often free, usually effective in removing most problem programs, updatable

-Cons: Require active control on user's part (user has to run it every so often), can mistake important files for spy-ware, require frequent updates

2. System Restores: built in system techniques for repairing damage to critical files. Most computers will come with a restore disk that is designed to bring the system's important files back to their original state.

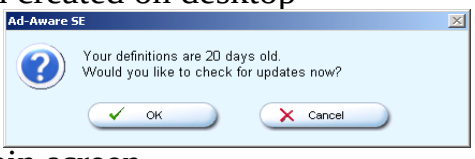
-Pros: Built in, sometimes customer/technical support will help you with it

-Cons: Not 100% reliable, will probably cause the loss of other things you've done, difficult

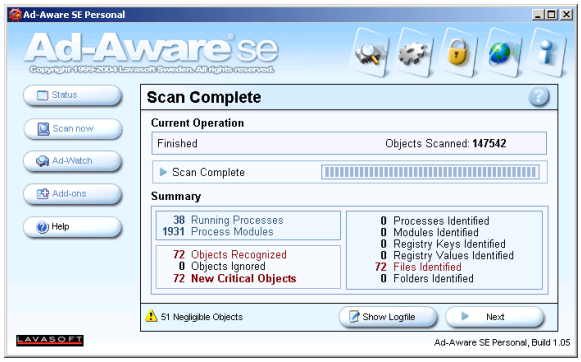
3. Manual Repairs: By this I mean, removing or repairing files by hand. Tasks like editing the registry, copying system files, etc. This is not for the casual computer user.

-Performing a Sweep:

1. Download installation file for Spy-Ware program (for today's example www.downloads.com then search for Ad-aware)
2. Save program to desktop
3. Install program by double-clicking on file on desktop
4. Double-click on program shortcut icon created on desktop
5. If prompted (→) update definitions



6. Follow prompts until you reach the main screen
7. Start sweep (left-click "Start" button for this program)
8. Perform full system scan
9. View the results



10. Select (left-click the boxes next too) all the files you want to have quarantined/removed.
11. Click the Delete/Finish/Quarantine button to remove files

Resources

http://www.spywareguide.com/

http://www.downloads.com

http://www.vmyths.com/

http://computer.howstuffworks.com/virus.htm

http://www.towson.edu/~jack/glossary/gloss.html

http://norton.com/