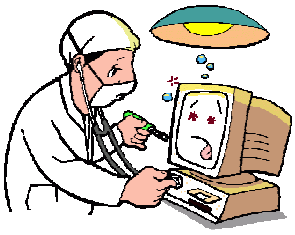
Malware Information:
Being Safe on the Internet

By Robert Osorio - IT Consultant, (352) 750-0845, Email: IhateMalware@PenguinBlog.com
Updated 3/13/14



Symptoms of Malware

Below are just a few symptoms that may reveal that you have malware operating on your computer.

- **Sluggish computer**
- **Strange icons on your desktop**
- **Fishy pop-up ads**: Pop-up ads from malware software are designed to look like they've been served up by the legitimate Web site you're visiting. As a result, you may not recognize them as a symptom of infection. There's no way to be sure, but if the contents of the ads seem strange - or if you're getting pop-up ads when you're not even surfing the Internet - then it's very likely that they are being served up by malware software installed on your computer.
- **Your default home page and search engine changes**: One of the oldest malware tricks is to automatically change your Web browser's default or start-up home page and search engine. This is the Web page that appears when you start your browser or click the "home" button.
- **Scary fake security warnings**: A popup window designed to look like security software, with frightening warnings about someone trying to attack your computer or spying on you and offering to "fix" the problems.

Malware Prevention & Safe Practices

Prevention is the key to protecting yourself from malware. While these tips will help you prevent malware, they are also examples of good habits that will help protect your privacy and security while online.

Keep in mind that most malware MUST be installed by YOU. You must give explicit permission. Thus the people behind these scams use social engineering to try to trick you into installing their malicious software. They may tantalize you with photos of celebrities, prey on your desire to give to charities, lure you with offers of free programs, or scare you with bogus security threats.

- **Read any popup window VERY carefully, and close it properly if it looks suspicious.** If a suspicious window or advertisement pops up on your screen that you suspect could be an attempt to fool you into installing a malware program, click the “X” in the upper right corner of the window to close it instead of clicking on the “No” or “Decline” button (often these buttons will only open another window in an attempt to annoy you into accepting the product, or the “Decline” button may actually be the “Accept” button in disguise). If you still can’t close the window, or others pop up to replace it, then shut down the computer and restart it.

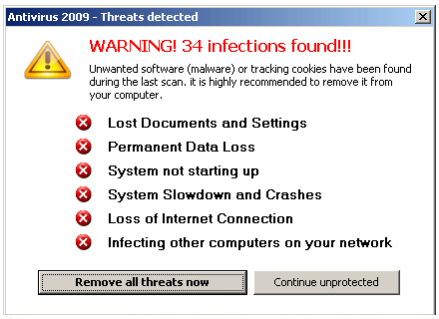
- **NEVER install anything you didn't ask for.** If you're on a website and something asks for permission to install, and you don't know what it is. SAY NO!

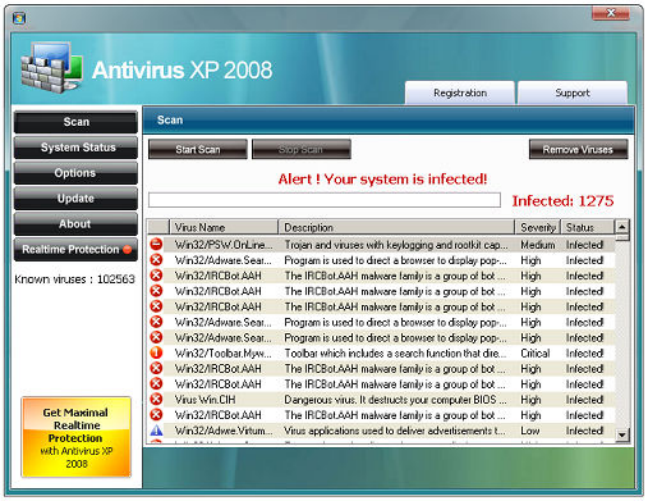
- **Be skeptical about installing strange or “free” software**: Make sure you know EXACTLY what is being installed onto your computer when you download applications off the Internet. Malware is often bundled with many free software downloads. Make sure you know what's in a package of software before you install it. Some "free" programs will install toolbars. Sometimes these toolbars are malicious. You do NOT need toolbars. Always read the installation prompts carefully and UNCHECK (opt-out) of any offers for toolbars. Free isn't always bad (there are lots of good free software) but free should make you wary. You should always do a Google search on the name of any free program you are thinking about installing. If the program is malicious, you will quickly find people complaining about it online.

- **Pay attention to security warnings**: Windows security warning screens alert users to new software being installed from Web pages they visit in Internet Explorer. You should not blindly accept say "OK" to these security warnings. Be sure you can trust the company installing the software. Make sure you are dealing with a reputable company and that you are actually on their website and not a fake website with a misspelled address (jcpennny.com instead of jcpenny.com for instance).

- **Beware of fake security messages.** Just because a security warning appears on your screen, it does not mean it's a legitimate message from your anti-virus program or Windows. It could just as easily be a fake pop-up made to look like a legitimate security warning. Be especially skeptical of messages designed to frightening you into immediate action (eg: "Someone is spying on you!" or "Your system is seriously compromised!" or "Someone is trying to access your credit card information!") and then asks you to "Click here to fix the problem". Your real anti-virus program will **never** try to scare you like this. Read the message CAREFULLY. Make sure the message is actually from your anti-virus program (for instance your real anti-virus may be called "Norton 360" but a fake security popup may identify itself as "Security 360" with a similar log to try and fool you). If it's not the same name as your anti-virus, then it's a fake. If in doubt click the "X" in the upper right corner. NEVER click on "No" or "Cancel".

Examples of fake security messages:





Dangerous Attachments

No one likes to hear this part, but let me be VERY clear: There are NO safe attachments or web site links you can open in an email. Let me repeat that:

THERE IS NO SUCH THING AS A SAFE EMAIL ATTACHMENT!

Period.

Email was originally designed to carry ONLY text information. Later on, the concept of attachments and links were added. Unfortunately these features were added at the expense of any security.

Email is inherently untrustworthy because there is no way to verify the sender. You have to use common sense to decide if you should open an attachment or click a link. The best rule of thumb is: if you weren't expecting it, don't open it.

For example, if you receive an email from your attorney with an attachment, and you weren't expecting it, then think twice. Does the signature at the bottom of the email look like the signature your attorney usually has in his emails? Is the body of the email vague? Are there glaring misspelling or grammatical errors? If in doubt, call your attorney and confirm that he actually DID send you an email.

NEVER open unsolicited attachments - even from friends. Malware authors love to use social engineering to trick people into opening attachments. For instance, slide shows are commonly used to carry malicious software. While you're watching the pretty slide show, a script may be running that installs malware if your computer has an un-patched exploit. These slide shows will be innocently forwarded to you by friends and family who have no idea they are helping criminals infect other computers. Don't help spread the poison! Don't forward these sorts of emails.

Another example: Fake emails from retailers may contain a file attachment that the email asks you to open to see your invoice. Before opening the attachment, you should ask yourself if you ordered anything from that retailer. Do you even KNOW who that retailer is? If in doubt, call them.

Another popular scam is fake emails from UPS, Fedex or the US Postal Service concerning an undeliverable package. Use you brain! These companies don't have your email address - they never ask for it when shipping a package.

Unless you're expecting it, DO NOT OPEN ATTACHMENTS!

This applies to web page links in emails as well. A common scam is an email claiming to be from a Facebook, a bank or Paypal saying there is a problem with your account, but to fix it "CLICK HERE". The link will take you to a fake web page where they hope you will enter your login information. BE SMART! If you don't have an account with this company, ignore it. If you do, then log in the way you normally would and check your account, or call them up. NEVER click on a link in an unsolicited email!

Don't "Friend" Me!

The above rule on attachments and links also applies to social networks like Facebook and Twitter. NEVER open links or attachments sent to you by friends on social networks. Sorry, it may spoil the fun, but it's the only way to be safe. It's very common for criminals to hack into Facebook accounts (people tend to use poor passwords that are easily hacked) and then send malware to all of that person's friends in the hopes of infecting them. This is also used in targeted attacks on employees of companies for the purposes of corporate espionage or data mining.

While we're talking about Facebook, think twice about posting ANYTHING that can be used against you by criminals. Assume EVERYTHING you post on Facebook is public. All it takes is one friend's account being compromised and the world will know everything about you. DON'T POST ANYTHING ON A SOCIAL NETWORK SITE YOU WOULDN'T POST ON A HIGHWAY BILLBOARD! Always assume NOTHING is private on Facebook or any other social networking site.

I would also recommend NOT filling out social network questionnaires. The questionnaire is made public so people can find you via common interests, but it also exposes you to great risk. Common questions include the name of your high school, date of birth, and where you were born. THESE ARE ALL COMMONLY USED AS SECURITY QUESTIONS BY YOUR BANK or other institutions in order to reset your password if you should forget it. Knowing these things, and your email address, is all a criminal needs to access your bank account or steal your identity!

Practice basic computer security hygiene:

- **Always use anti-virus software**: And keep the software up to date. Over 500 new viruses are discovered each month. You are not just protecting yourself when using anti virus software, but also others you communicate with.

  You can download Microsoft's free Security Essentials anti-virus from http://*windows.microsoft.com/mse*

  For extra protection, you can pay for a more pro-active security program like ESET Nod32 or Kaspersky (they can be purchased online as downloads). I do not recommend McAfee or Norton since malware authors know these are the two major anti-virus vendors, and as such their malware is designed to beat them. I prefer to recommend anti-virus software that's "off the radar".

  ESET Security: http://*eset.com*
  Kaspersky: http://*kaspersky.com*

- **Keep your Windows operating system up to date**: You should always make sure that the Windows operating system on your computer is up to date with the latest security patches from Microsoft. Make sure Windows Automatic Updates is enabled (it's enabled by default).

- **Keep Adobe Flash and Adobe Reader updated**. These are necessary programs used by your computer to browse the web. They are updated monthly to fix security flaws. Make sure they are configured to update automatically (the default). You can download the latest versions of Adobe Flash and Adobe Reader from *Adobe.com*

- **Do not install Java.** If Java is installed, uninstall it. Most people do not need Java (and if you do need it, you'd know). Java security flaws are the number one source of drive-by infections. If you must use Java, make sure you keep it up to date (a balloon message over the Java icon in the taskbar will notify you if an update is available). You can download the latest version of Java from *Java.com*

- **Beware of fake Flash or Java update popups.** Clicking on these may install malware instead. If in doubt, go directly to *Adobe.com* to update Flash and *Java.com* to update Java.

- **Beware of "free" programs**: While not all free programs are malicious, many are, and many "free" programs are not actually free. The price is sometimes allowing some advertising malware to be installed on your computer that nags you with advertisements, or tracks your browsing habits on the Internet, or (as in the case of rogue security software) extorts you for money.

- **Beware of additional payloads**: When installing legitimate programs and updates, there will often be a free toolbar included (for instance Java updates try to install a toolbar). The toolbar may not be malicious (Google, Yahoo, MSN toolbars for instance) but it might be annoying or may slow down your browser and is certainly not required. Legitimate software will usually give you the option to "opt out" of installing the toolbar by un-checking a box during the install process, so read each screen carefully.

- **Do not overly rely on your anti-virus program**: Anti-virus programs are not perfect. New threats are being discovered all the time and there is often a delay between the time a new threat is discovered, and your anti-virus program is updated to recognize it. Also many malware programs exist in a legal "gray area" and your anti-virus may not be able to legally block it if you gave your approval to install it. **Safe browsing habits are your first line of defense!** Your anti-virus program should only be a last line of defense.

- **Use Mozilla Firefox or Google Chrome instead of Internet Explorer**: Firefox is a free web browser available from *Firefox.com*. Chrome is another free web browser available from *Chrome.Google.com*. Both work just like Internet Explorer but are MUCH safer. They do not replace Internet Explorer, and you can have multiple web browsers installed on your PC and open any one you want. Both Firefox and Chrome will offer to copy over your favorites (they are called Bookmarks) for you automatically.

Why Do People Write Malware And Viruses?

MONEY. Pure and simple. This is not for fun anymore, it's for profit. Malicious software is a multi-BILLION dollar industry, run by organized crime.

How does it work? Well let's assume someone can make just ONE DOLLAR by infecting a single computer with a virus or malware. Then assume he can infect 10,000 computers a month. That's $10,000 a month!

What's worth so much on your computer? Sure passwords, social security and credit card numbers are used for identity theft, but this is small change in the criminal world. Sorry to say, but your credit card number is only worth a few dollars on the black market.

Selling you something you may THINK you need, which you don't really need is also profitable: fake security software, fake registry cleaners, programs that claim to "speed up" your computer.

Even more valuable is INFORMATION. Personal information about your browsing habits is extremely valuable to marketers both legitimate and shady.

Your computer is also valuable all by itself. Trojan horse (trojan) programs are designed to take over your computer without giving themselves away. Usually the only way you can tell if there is a professional trojan on your computer at all is if it's running slow. While you are typing a letter or browsing the Internet, the trojan may be using your computer (along with hundreds of thousands of other infected PCs) to send SPAM, attack corporate or government websites, or store illegal files like child pornography.

Targeted attacks are becoming more common as well. They may not be interested in YOU specifically, but they may want to take over your computer to see if it contains information about the company you work for, people you know, or just to fake your identity to take advantage of someone else.

More Information on Safe Web Browsing:

http://GetNetWise.org

http://SafeSurfingKids.com

http://SecureFlorida.org

http://Microsoft.com/security

http://onguardonline.gov/articles/0011-malware