



this issue

The Rising Plague of Malware **P.1**

Upcoming Events **P.1**

Trends & New Software **P.2**

Upcoming Events

CT Thanksgiving

Join us for a Thanksgiving Lunch
Open House.

Date: Thursday Nov. 19, 2009

Time: 11:00pm -1:00pm

RSVP to 262-789-8210 or
register@ctaccess.com

We are collecting donations for a
local food pantry. Please help us
by bringing non-perishable food
items or a cash donation.

THE RISING PLAGUE OF MALWARE



**Scott
Hirschfeld**

We are not flashing back to 2002. Spyware, also known as malware, adware, scumware or snoopware is still here in 2009, and unfortunately the threat, instead of being pushed back over the years is only increasing. It is likely, even with protection strategies in place, that you have had to deal with cleaning up the mess malware has left behind. If you haven't had to deal with the expensive cleanup, it is possible you may have malicious code installed on your system and are not aware of it.

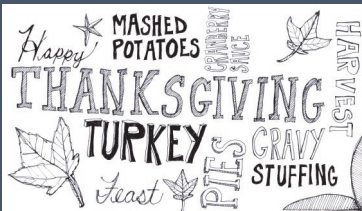
McAfee has identified over 1.2 million unique types of malware just in the first half of 2009. This is more than double that reported in the first half of 2008. Malware transmits itself to a local PC as one browses the web. Hackers break into legitimate websites and implant the code. When a user searches for some topic on a search engine like Google and then clicks to go to that site, the code downloads itself and infects the PC (sometimes without the user noticing), unless there is something to block that download. Google reports that in 2009 the number of entries on their infected list has more than doubled, with periods during the year where 40,000 new websites were compromised in a week's time.

So, we have established that there is more Spyware out there, but why is it important? When spyware first began to weave its way around the web, it was often considered a prank or an attempt by some over-geeked student to make a name for himself. This is certainly not the case anymore. The singular goal of spyware is to compromise security by either finding or transmitting information stored on your PC to be bought and sold, or by actually giving remote control over your PC to other users.

Hackers are getting paid large sums of money for control over groups of compromised PCs, or for lists of credit card numbers. The techniques used to create and maintain these infected groups of PCs, or "botnets", are as professional as those of a large corporate software developer. Once information is gathered, it is bought and sold covertly through networks such as the recently uncovered, Golden Cash network.

What measures should be undertaken to prevent your business from being compromised?

It is no longer good enough to instruct your employees to avoid questionable websites. Even if an employee could determine what types of sites were questionable, legitimate websites





have been compromised by malware. This makes some method of proactive prevention necessary. Some anti-virus software manufacturers have begun to include anti-spyware protection, but in most cases it is limited. It is still better to implement a separate strategy for blocking malware.

There are two proactive ways to block malware. Neither is full-proof, but both put you in a much safer place than ignoring the problem. The first method is with corporate malware prevention software. This software installs on each PC on the network and works very similarly to your anti-virus software, blocking the spyware as it tries to download to your PC. Webroot Spysweeper is an example of one such software program that does a good job. Beware of downloading anything off the web for spyware prevention as often these programs are malware themselves.

The second method of preventing malware is with a gateway spyware blocker. This is an add-on for newer firewalls that screens the malware out before it gets to your PC and blocks it from entering your network. The advantage here is that the malicious code is blocked at the entry point! If your firewall does not have this feature as an add-on, it may be time to upgrade your firewall.

In addition to implementing some type of spyware prevention tool, it is also very important to keep your system up-to-date. Firewalls are only good if the software on them is updated regularly to identify and block new types of attacks. Microsoft's Internet Explorer is the entry point for most spyware. Updating Explorer to the latest version that includes all sorts of security enhancements is important. Loading all of the Microsoft security updates and enhancements is also recommended to keep

your system as safe as possible. Some even recommend using an alternate browser like Firefox or Chrome which are reportedly less susceptible to malware.

It may also be advisable to consider upgrading to Windows Vista or Windows 7 for improved security at the PC level. Taking away local administrator privileges from your user accounts, so that no software can be installed on the user's PC may also help in staving off the flood of spyware.

If you suspect that you may have some sort of malware, there are several tools available out there to help cleanup. The free tool that seems to do the best job of cleanup is Malwarebytes. This tool can be safely downloaded from Cnet's



download.com. The important thing to remember is that if you suspect that your system has been compromised by a true "botnet" type piece of

code, the only way to be sure that all of the threads of the spyware have been removed is by reloading your system from scratch.

Unfortunately malware is a reality of our interconnected world of technology. The open framework of the web is what makes it great, but also what brings these dangers. Because many of these threats come from overseas, it is difficult to track down and enforce the laws already in place to stop the activity. I expect malware will continue to be a problem, but with the proper prevention we can continue to take advantage of the web and stay safe!

Scott Hirschfeld is Vice-President of CTAcess/Computer Technologies of Wisconsin. If you would like more information on spyware, malware and how to best protect your network, please contact Scott. scott@ctaccess.com or 262-789-8210

EYE ON IT Cool Tools

There is a great new hosted solution for transferring, storing, and sharing files. From simply transferring files between home and office, or posting files for others to access over the Internet to full featured online collaboration including task assignments and discussions, box.net may be the solution for you. They have several different plans starting with a free version for individuals and students to use for personal file sharing to the Enterprise version that gives you administrative oversight and custom branding. For more details and pricing information go to www.box.net.

SOFTWARE Monthly Picks



You might want to try VLC Media Player, if you are having problems with the media player that came with your pc or laptop. VLC is a free and open source multimedia player that supports most audio and video formats from files and DVDs to streaming protocols. It can also convert files and act as a streaming server. For more information or to download go to www.videolan.org/vlc.

Spyware Symptoms

With 9 out of 10 internet connected pcs infected with spyware, it is very likely there is some form installed on your computer. If you recognize these symptoms, you may be infected:

- Sluggish performance
- Increased pop-ups
- Mysterious new toolbars you can't delete
- Puzzling search results
- Frequent computer crashes
- Unexplained changes to homepage settings