Common Malware Threats

By now everyone has heard the terms "malware" [http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci762187,00.html], "adware" [http://searchSmallBizIT.techtarget.com/sDefinition/0,,sid44_gci521293,00.html], "spyware" [http://searchCRM.techtarget.com/sDefinition/0,,sid11_gci214518,00.html] and maybe even "crapware." What are they, what are the top threats and how do you identify and defend against them?

Briefly, adware is a small program that presents advertisements to you on your computer. The distinction between adware and a web site with advertising is that the web site's ads are server-side while the adware ads are client-side, though the end result may look the same to the user since some adware hijacks your browser and inserts ads that do not exist on the actual site. Spyware is similar, except the purpose is to monitor your activity in some way, perhaps by tracking your browsing or on-line purchasing habits or more seriously, capturing keystrokes when you log into a financial institution.

Malware and crapware are more generic terms that encompass both of the above, and may also include other malicious code like viruses, worms or Trojan horses. Some malware may also be considered a Trojan in that it claims to be one thing but is really another. Other malware, especially adware, tells you what it is, but the description may be buried in legalese or otherwise non-intuitive or difficult to spot. But the most dangerous malware can install itself without user knowledge or intervention. This is sometimes called a "drive by download" [http://whatis.techtarget.com/definition/0,,sid9_gci887624,00.html, see also Five malicious code myths -- and how to protect yourself in 2005 [http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1041736,00.html].

Malware, like spam, exists because someone saw a hole and a way to make money and others copied it with abandon until we got to where we are now. I do not have hard numbers to back this up, but anecdotal evidence suggests that the problem has gotten significantly worse since November 2004. The risk from malware runs the gamut from the merely annoying (ads), to the very serious (identify, financial or information theft) and everything in between. One peculiar aspect to malware is that it is often written very poorly. It may often crash, or interact poorly with other software or other malware. A machine that is vulnerable will continue to attract malware until it collapses from the load and malware programs fighting each other, which helps the Internet but is not so good for the user and system administrator that has to fix it.

And this is one case where we can't blame the user. You still need your policy and user education, but in it is entirely possible to pick up malware even with strict firewall rules and anti-virus in place, fully up to date patches, and a decent case of paranoia. How can this happen? Internet Explorer, ActiveX [1] and Browser Helper Objects (BHO) [2]. I frequently characterize IE as the most insecure piece of software on the plant, and ActiveX and Browser Helper Objects are a large part of the reason. They both fundamentally, inherently, allow someone to write a small piece of code that can be transparently downloaded to your computer where it can do anything you can do. This is not something that can be fixed, it's what they were designed to do. Does that sound like a good idea to you?

ActiveX does essentially the same job as Java, and BHOs are essentially the same as Netscape or Mozilla plug-ins, so the concept is not inherently bad, but the implementation and lack of controls is. That is also not to say that IE is the only vector for malware or that other browsers such as Firefox are immune. Instant Messaging clients are another vector for malware, and all other browsers have flaws, more of which wil be exploited as alternative browsers become a bigger target.

So how do you detect malware? One of the easiest, though not recommended ways to find out you have malware is when your machines slows to a crawl, constantly crashes or doesn't work right, or barrages you with popup ads. If a normal Google search produces a page of ads before you get to the actual results, if IE works but Firefox doesn't or IE works more poorly than usual, those are strong signs of malware.

Obvious signs like that aside, it isn't easy. Most malware goes to great lengths to be downloaded, installed and run invisibly and it can be very difficult to remove. Your best bet is to not be infected in the first place, and that's easier said than done too.

Content filtering at your firewall, proxy server, mail server and possibly via an Intrusion Prevention System (IPS) may help, but its very difficult to remove all malicious content in all of those places without affecting legitimate business activities.

Various type of egress filtering will block the spread and in many cases the effect of malware, but only after you are infested. You can create hosts files (or DNS records) that resolve known malware servers to localhost or create a malware blacklist of sites to block at the firewall in addition to your regular egress filtering [4] (you **are** doing that, right?**)**. One interesting twist is using egress filtering on your computer itself. That's the reason I love ZoneAlarm—it tells me what programs on my computer are accessing the network, though malware often tries to look like regular operating system files for this reason. When in doubt, Google it -- if there is any question about the legitimacy of the program, the top 10 Google hits and sponsored links will clear it up.

While current anti-virus programs will not help [5], that may change in the future and there are already many commercial and free anti-malware products [6] from small companies and large (e.g. Microsoft, McAfee and Symantec). These products tend to fall into two main categories, inoculation and detection/removal. Innoculators [http://searchwin2000.techtarget.com/tip/0,289483,sid1_gci969259,00.html] such as Spywareguide.com try to prevent malware from being installed in the first place, via the ActiveX kill bit, and similar means. Detection and removal products help you clean up after the fact. If you suspect a malware infestation (and even if you don't) I strongly suggest running two or more products, as each product often finds different things.

Finally, you should consider using any browser but IE. Switching browsers is non-trivial at enterprise scale, but it well worth consideration. Since Microsoft has focused all their attention on XP and Longhorn, they are neglecting the older versions of IE used on the Windows 9x, NT and 2000 platforms still in widespread use in the SME environment, so in this case it's a no brainer. Vastly reduced vulnerability to malware aside, the pop-up blockers and tabbed browsing available in all other major browsers is well worth it.

In closing, I'd like to say that I think Microsoft is throwing away a golden security and PR opportunity in not supporting anything older than Win2000 in their Anti-Malware and Anti-Spyware products [7]. I understand the product lifecycle and support argument but if MS was **really>** concerned about security they'd help secure the millions of copies of those older systems still out there in the SME environment. Here's my contribution, a quote for the press release:

> "While these platforms are officially unsupported, we recognize that they are still in widespread use, so in an effort to increase the security of these systems these tools may also be used on them."

[1] http://msdn.microsoft.com/workshop/components/activex/intro.asp
[2] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp
[3] http://searchwin2000.techtarget.com/tip/0,289483,sid1_gci969259,00.html
[4] http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci883409,00.html and http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci838215,00.html
[5] Some A/V vendors "were reluctant to even touch adware because user consent raises liability issues over treating it as malware." http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1030076,00.html, http://www.google.com/search?num=30&q=Weatherbug

[6] http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1043496,00.html
http://searchsecurity.techtarget.com/search/1,293876,sid14,00.html?query=malware&ctype=ALL
http://www.google.com/search?num=30&q=malware+OR+spyware+OR+crapware
[7] http://www.microsoft.com/security/malwareremove/default.mspx,
http://www.microsoft.com/athome/security/spyware/software/default.mspx

Anti-malware Products

(As of February 2005)

Product Name	**URL**
AdAware	http://www.lavasoftusa.com/software/adaware/
Spybot	http://www.safer-networking.org/
BHO Demon	http://www.definitivesolutions.com/bhodemon.htm
Spyware Blaster	http://www.javacoolsoftware.com/spywareblaster.html
StartupMonitor	http://www.mlin.net/StartupMonitor.shtml
MS Malware	http://www.microsoft.com/security/malwareremove/default.mspx
MS AntiSpyware	http://www.microsoft.com/athome/security/spyware/software/default.mspx http://www.pcworld.com/reviews/article/0,aid,119300,00.asp (Review)

Suggested links in no particular order (includes footnotes but not anti-malware products from above)

(As of February 2005)

Investors Supporting Spyware	http://www.benedelman.org/spyware/investors/
Browser Helper Objects: The Browser the Way You Want It	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp
Introduction to ActiveX Controls	http://msdn.microsoft.com/workshop/components/activex/intro.asp
BHO's- Browser Helper Objects	http://www.spywareinfo.com/articles/bho/
The threat of Browser Helper Objects	http://www.zdnet.com.au/insight/security/0,39023764,39153405,00.htm
Spyware Reviews - January 2005	http://www.adwarereport.com/mt/archives/000004.html?SOURCE=goog&KEYWORD=malware
Spyware Removers 2005 - Overview	http://www.spywareremoversreview.com/
Is Windows AntiSpyware a good fit for enterprises?	http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1043496,00.html
Five malicious code myths -- and how to protect yourself in 2005	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1041736,00.html
Rousting spyware	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1030076,00.html
Windows XP SP 2 -- Helps control malware ... but watch out for that firewall!	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1012627,00.html
Guarding against malware infection from remote users	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1003489,00.html
Ditch IE?	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci996634,00.html
Blocking spyware via the ActiveX kill bit	http://searchwin2000.techtarget.com/tip/0,289483,sid1_gci969259,00.html
Egress filtering	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci883409,00.html
Firewall best practices	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci838215,00.html
First Look: Microsoft AntiSpyware	http://www.pcworld.com/reviews/article/0,aid,119300,00.asp
ActiveX - my experience	http://bookofhook.com/phpBB/viewtopic.php?t=387
Blocking Unwanted Parasites with a Hosts File	http://www.mvps.org/winhelp2002/hosts.htm
Using the Hosts File [to block malware]	http://www.accs-net.com/hosts/
Search searchsecurity.techtarget.com for malware	http://searchsecurity.techtarget.com/search/1,293876,sid14,00.html?query=malware&ctype=ALL
Search Google for malware, spyware and crapware	http://www.google.com/search?num=30&q=malware+OR+spyware+OR+crapware