The Security Geek – An Occasional Newsletter.

In spite of the whimsical title of this newsletter, computer and internet security is no casual matter. The threats – viruses, worms, trojans, malware, spyware, operating system exploits, network exploits – multiply at Malthusian rates while the tools to fight those threats seem as outdated as those Troy deployed against the Greeks and the original Trojan Horse and not at all like the high-tech tools needed to stop the flow of the electronic Trojans delivered daily to your email inbox. Well, all the tools seem outdated except one, knowledge, and with that tool we can fend off most any Greek hoard.

To that end let's start this knowledge course with some definitions.

A ***virus*** is a specially crafted computer program that resides inside a host program. When you open or run the host program the virus is triggered and infects your computer. The significance of this is that under most circumstances, unless you run the file you cannot get the virus – that is you must do something to get the infection. Today, most viruses are spread via e-mail attachments – hence the common suggestion to never open an e-mailed file without first talking to the sender.

A ***worm*** is a specially crafted computer program that exploits a flaw in another program, most often in the operating system. Worms are particularly pernicious because they spread without user intervention – that is you do not have to open or run a file to get a worm. If your computer is running the targeted operating system or program and you connect to another computer that already has the worm (typically on the internet), you will automatically and immediately become infected. The only real protection against worms is to update your software frequently.

Trojans are files that look innocent from the outside but contain malicious code inside. Most viruses are trojans as they spread by enticing you to open the innocent looking wrapper, though worms, typically, are not as they spread without your help and so do not need a disguise. Spyware is also a type of trojan.

Spyware has come in for a lot of attention of late, and deservedly so as it is the fastest growing source of computer security issues. At its most basic, spyware is software or pointers installed on your computer that transmit information about how you use your computer to some third party. This is not always evil or bad. When you go to a site like The New York Times or The Wall Street Journal it may be to your advantage if they know who you are so they can automatically complete the login process, allowing you to read articles without interruption. This can be enabled by loading a cookie, or text file that uniquely identifies you, on your computer. Most cookies are safe. However, other types of spyware can be quite dangerous.

Some spyware tracks not just your time at one site, but at all sites and then sends this data back to a third party who can use this information to target you for unsolicited sales material. While not a particularly evil thing, if a program is doing this without your permission it is certainly an invasion of privacy. Other spyware goes even further. Some spyware programs will change your system settings, forcing you to use their search engines, start-up or home pages, only allowing you to visit certain sites, repeatedly opening browser windows with advertising (most often for gambling or pornography sites) and worse. Ok, what's worse than dozens of windows automatically and uncontrollably opening with porn ads? How about a spyware program that senses when you are making an online purchase and then records your keystrokes, capturing your credit card information, and then sending that information on to an unauthorized third party!

These latter types of spyware – programs that change settings and record information are also called ***malware***, or malicious software. Bad spyware certainly is malware and the terms are often used interchangeably, though technically they are not the same as malware also refers to any software that has an out and out bad effect on you and/or your computer and so also includes viruses and worms.

The reason to identify these terms is so that we can discuss security with greater precision. For example, since viruses spread by infecting a host program, you can avoid nearly every virus by not opening unfamiliar files. And if you are infected by a virus, the Security Geek will know that you, personally, took an overt action you ought not have.

On the other hand, if you are infected by a worm, there is a possibility that there was nothing you could have done to prevent it as worms spread without your participation – though if the worm exploits an older, known flaw in Windows, for which there is already a posted patch the Security Geek will know you are not maintaining your computer properly.

Similar to a virus, the vast majority of spyware requires action on your part. But where a virus is typically a part of an email attachment, spyware is usually part of a larger program that you install on your computer. For example, you may see an online ad for a "free" screensaver and install it. And you will get that screensaver, but the screensaver code may also include a spyware program that automatically refers you to their affiliate search engine – or worse. So if you have a spyware issue, the Security Geek will know you believe in the free lunch theory and have tried to get something you think valuable for no cost to you whatsoever.

Alright, enough background knowledge for now, let's turn this brain power into action to help protect your computer and data from internet based security problems.

Anti-Virus Software

The first thing every computer user should install (besides the operating system) is an anti-virus program. There are a half dozen or more AV programs available, and the differences between them are nowhere as large as their marketing departments would have you believe. In fact, most of the larger AV firms cooperate behind the scenes, informing each other of new threats immediately, so the likelihood of one program finding a virus and another not being able to is pretty small. What does differ is their interface and ease of use. Here in the office the Security Geek prefers Norton AntiVirus by Symantec. The reason is simple, their interface is easy and installation is a snap. Further, their update process is automated. Why is that important? Because a computer virus, just like a human one, is at its most dangerous when new. If you have an anti-virus program on your computer but have not updated it in a month, then it cannot protect you from any virus younger than that just as last years flu shot will not protect you against this years flu. Norton updates every Wednesday as well as periodically throughout the week if there is an especially virulent new virus. Other companies that make excellent AV software are McAfee and Panda Software, but please keep in mind that it is an office policy that all computers used in the office run Norton.

This is good spot to introduce a special topic, social engineering. Social engineering, as it applies to computer use, is the attempt to get you to do something you know you should not. Like, say, opening an e-mail attachment.

Actually, I admire many of my fellow geeks for their skill in social engineering. Yes, I know geeks are unsociable misfits, but they still find pretty insightful ways to get you to open attachments. One of the first and perhaps the most brilliant piece of social engineering was the "I Love You" virus. By simply calling the attachment I Love You, millions of apparently lonely folks opened a file to see whom it was from. A more recent virus included a message that your e-mail had bounced and included a code. The message went on to say that you would need to use the code to open the attachment. Since this looked all very official – after all, who would send a code unless it was on the up and up – people went a head and did exactly what they had been told not to do. See, we geeks are both more human and more insightful than you thought!

Another piece of social engineering written in to most recent viruses is how they use your computer to spread themselves. Most viruses will e-mail themselves to everyone in your e-mail address book. But rather than use your name as the sender (if it did this, the first person to get the infected e-mail could call you and have you run your AV software and wipe the virus out) it grabs a random name from your address book and uses that as the sender on the gamble that most of the people you know also know each other. This way, the virus comes into person A's computer, grabs the name of person B and sends itself to person C, who knows B and so trusts the attachment and opens it. A colleague of mine had his network taken down several weeks ago when a user opened an attachment, supposedly from the president of their main software vendor. So, need I say it again? Do not open unsolicited attachments!

Worm Defense

How do you protect against worms? Simple, update your software. Often.

If you use Windows, the easiest way to do this depends on the version of Windows you are using. If you are still using Windows 95/98/ME (though I have no idea why you would be as these versions of Windows are highly unstable and insecure), open the control panel and select the Automatic Updates icon. From there select the third option, “Automatically download the updates, and install them on the schedule that I specify”, and then select, “Every day”, and a time when you are typically on the computer.

If you are using Windows 2000/XP you can get to the same selection screen by right clicking on My Computer and selecting properties. One of the tabs will be, “Automatic Updates”, and by clicking on it you can see the same option indicated above.

However you select automatic updates, you would still be well served to occasionally run the Windows Update by itself. This you can do by selecting the Tools menu in Internet Explorer and then Windows Update. The Windows update site is pretty self-explanatory, so I won’t go into detail on how to use it but I will point out that any critical updates you see you should immediately download. In the Windows update section you should also select any “recommended” updates. And in the Drivers section, please download any item there as well. Lastly, from the Windows Update screen you can get to the Office Update site (the link is close to the top of the opening Windows Update page). Office update will repair security and program flaws in Microsoft Office programs (Word, Excel, Outlook, Publisher, etc.) in much the same way as Windows Update fixes Windows. While not as critical to your computers security as Windows Update, the fixes to Outlook, if you use it, are of particular import and should be installed immediately.

Before we leave worms, here are a couple of additional items to keep in mind. The newest generation of virus and worms use “blended” threats, that is they combine worm and virus attributes. So, instead of having only one way to attack, they use multiple vectors. A virus may fold itself inside an attachment and then once inside your computer use a worm to infect your operating system – or a worm may exploit several flaws in Windows (though it only needs one to get inside) and then once in can pull virus and/or spyware like programs from the internet on to your computer. These newest pieces of malware are particularly hard to defend against since you may have protected yourself from one attack vector only to have a lapse in another and then – WHAM – you get it in all areas. This is why you must be diligent about updates to your operating system as well as AV software.

Second, most worms exploit already patched holes in Windows. In the Geek business we use the term X-day exploit. That is, when a new worm is released we give it an additional name based on the interval between the day the flaw was revealed and a patch made for it, and the worms arrival. The Code Red and Nimda worms from several years ago were 331-day exploits, that is it was almost a year from the time Microsoft released a patch to the time someone wrote an exploit based on that flaw. The fact that that worm caused so much damage woke up many in the IT industry to the need to remain up to date on patches. But it gets worse. The Slammer worm was a 180-day exploit, meaning that the worm writers delivered that piece of code in half the time of Nimda. Blaster, which surfaced last February, was a 25-day exploit. And MyDoom, which arrived a month or so ago, was a 0-day exploit. Ok, what is a 0-day exploit? It is a worm that attacks a problem for which there is not yet a patch! Yes, that is scary as it is possible for you to get a worm from which you cannot protect yourself. And this means you need to pay attention to the news. When you hear of a new worm, listen carefully. If there is not a patch for it, use the internet with extreme caution until there is a patch in place as you usually get worms without knowing it.

Spyware

Spyware works best when it is low profile and when it exploits a person’s sense of greed. How’s that? Well, if it keeps a low profile you may not know you even have loaded a piece of spyware and hence will not remove it. And the best way to get you to install it in the first place is to offer you something that you think is valuable for free.

Most spyware is loaded from the internet as a “helper” program, that is as a program that while not a full-blown application like a word processor or spreadsheet, helps you with the little things. Like a weather monitor, or a screensaver, or a desktop wallpaper program, or “fun” cursors, emoticons or fonts, or a small calendar, or perhaps worst of all, an additional toolbar for Internet Explorer. Most of these programs are “free” and so seem like a pretty good deal. But stop. How can anyone make money by giving stuff away? Can you? So why should you be able to get really cool, fun and useful programs for free?

See what I mean by exploiting greed.

The problem is that these programs are not the mythical free lunch they pretend to be. Nearly every single free helper program on the internet is really a piece of spyware. Some are very well written and so do little to show their presence, others are so poorly coded that within hours of installing them your computer will become unusable, perhaps to the point of having to be reformatted and rebuilt just to regain control.

The first solution to spyware is not to get it. Like a virus, you can only get spyware by cooperating, that is by pressing a button on your computer. But, if you have pressed that button, there are two excellent tools to help your recover your computer – the odd thing is that both violate the free lunch rule.

Ad-Aware and Spybot Search and Destroy are both programs that you can download from download.com (the Security Geek loves the internet when it’s literal). Yes, I said that free programs are usually bad, but these exceptions to the rule are essential tools in fighting spyware – even Microsoft themselves recommend using them – and if you can’t the trust the word of the richest convicted felon in the world, who can you trust?

I suggest that you download Ad-Aware first, and run it. Keep running it until you find zero spyware. Then download Spybot Search and Destroy, keep running it until you find zero spyware, and then immunize your system with it. Combined, these programs will trap for, find and remove about 90-95% of all spyware. If, after following these procedures you still have spyware issues there is another program out there that will most certainly clean your system, HiJack This, but if you misuse in any way your computer may refuse to even start up.

Done, Sort Of

In this first issue of The Security Geek we have briefly (believe it or not) highlighted some major program based threats to your computer from the internet. In the next issue, we will highlight network-based threats such as intrusion and eavesdropping. In the meantime, I’m hopeful that after reading this you will be more vigilant then the defenders of ancient Troy were. The threats are real. I have examined computers that have had over 1000 viruses on them as well as some that had over 3000 pieces of spyware. According to Panda Software, about 25% of all computers in the US, at this exact moment, have a virus. Armed with this knowledge there is no need for you to become one of the statistics.

/Geek Out