;login:

THE MAGAZINE OF USENIX & SAGE

August 2003 • volume 28 • number 4

inside:

USENIX & SAGE

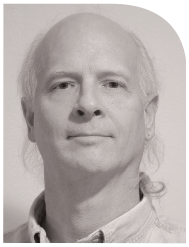
The Advanced Computing Systems Association &
The System Administrators Guild

musings

by Rik Farrow

Rik Farrow provides UNIX and Internet security consulting and training. He is the author of *UNIX System Security* and *System Administrator's Guide to System V*.

rik@spirit.com



A funny thing happened to me last May. I was asked a question about Microsoft Windows desktop security that actually caught my attention.

In a single week, two women contacted me wanting to know how to stop their ex-boyfriend from reading their email. I immediately thought of a trojan running a keystroke logger and suggested that they get, or update, their antiviral software. But then I decided to look further.

I didn't have very far to look. Just enter "keystroke loggers" into a Google search, and you will turn up thousands of entries, as well as sponsored ads for spyware, the more common name for keystroke loggers. Based on the advice of compadres in the world of security more familiar with Windows, I pointed both women to SpyCop, a spyware detector. But I didn't stop there.

As I continued to search, I found a site (*http://spywareinfo.com*) that listed 223 spyware products (this is actually an anti-spyware site). Another vendor stated that there were over 300 spyware programs available. I found a hardware dongle (Keyghost) as well as a number of spyware detectors.

Spyware, in the generic sense, is nothing new. Microsoft made headlines when it included a mechanism to scan hard drives for software and upload those listings with pre-release versions of Windows 95. Microsoft quickly removed that feature. But current versions of Windows Media Player contact Microsoft every time you play a CD or DVD, to collect a track listing for you. Unscrupulous programs could, in fact, log that data for later reference or analysis (a unique ID is registered for each copy of the WMP).

And spyware for X Window has been around even longer than Windows. You can search for and find versions of the xkey program, an X client that collects all keypress events in any X Window server it can connect to. Of course, you are protecting your X Window server (it appears that any reasonable UNIX distribution uses xauth, but X Window for Windows products often fail to do this). One weakness of xkey is that it reports all keypresses, without identifying the application reading those keys. X events do include a window ID, and it should be possible to actually match keys with applications with a bit of programming.

Note that someone who adds a line to a UNIX user's startup files can run xkey as that user and will have complete access. Protect your dot (startup) files!

But Microsoft makes things much easier for Windows programmers, one of the reasons for Microsoft's phenomenal success. Just as personal firewall products for Windows can identify which application has requested a network connection, keystroke loggers for Windows can identify the application that will receive any keystrokes. That made it possible for the Badtrans.B trojan to focus on the characters presented to particular applications, such as Telnet and connections to RAS (Remote Access Servers). A similar keystroke logger helped someone invade Microsoft's networks in the summer of 2000 by capturing a username, password, and RAS server address.

Anti-spyware products often work like antiviral products, looking for signatures. Another sign of a spyware installation is changes to certain registry keys and startup files. I have been told that there are at least 56 different methods that a trojan writer can use so that the trojan gets restarted with every reboot or login. The most common ways include modifications to the various Run keys in the registry, to startup files like WIN.INI, and to users' startup folders. You can actually download a free program

If only George Orwell (*1984*) had known about PCs, it wouldn't have been the TV watching its viewers.

from Sysinternals (*http://www.sysinternals.com/ntw2k/source/misc.shtml#autoruns*) that will report on the list of all software started with each reboot, including services. Installing a "special" service, such as slanret, has become a popular way of rootkitting Windows 2000 systems, so you do want to pay attention to the .sys files included when your system boots. Microsoft wants you to stick to signed drivers, which should help you avoid being rootkitted.

And if you are wondering about how someone installs a keystroke logger, a common way to do it is through physical access. But Windows viruses and trojans will also do this. Note that the virus Bugbear.B, which was making the rounds in early June, uses as one of its vectors the MIME-auto-exec bug that Microsoft announced a patch for in March 2001 (*http://www.microsoft.com/technet/security/bulletin/MS01-020.asp*). Bugbear.B also uses a more recent, just patched, vulnerability in Internet Explorer to execute its code. If you use IE, check for patches often.

As I learned just how common spyware has become, I wondered about the legality of it. I heard from a police dispatcher, for example, about a father who had installed spyware to monitor his daughter's Internet usage. So I contacted an acquaintance within the US Department of Justice who deals in computer crime and asked him if he could help me. He agreed, but only as a background source.

Using spyware without authorization is a federal crime, a felony in the US. But that word, "authorization," is the slippery one. Your employer is authorized to sniff your keystrokes or network connections if you have agreed to a policy that includes monitoring or the systems you use have logon banners announcing that use amounts to an agreement to be monitored.

Parents have been given a free ride by the courts when they are acting as responsible custodians for their children. But an ex-boyfriend, girlfriend, or husband who installs software that collects electronic communications would be considered to be committing the same offense as tapping a telephone (the same laws apply). Same thing when someone, without permission, installs spyware in your computer to collect keystrokes. My Justice Department contact told me that if that information were used to break into a computer, he would be more likely to use the break-in during a prosecution, because it would be easier for a jury to comprehend than keystroke logging.

But keystroke loggers are not the only applications spying from within Windows desktops these days. Many "free" services include clauses within the EULAs that permit them to install software that monitors Web usage, music tracks downloaded, and so on, all the better to target the user for advertising and spam. And this is an authorized use, because the end user agreed to the EULA. Kazaa users beware!

In these scary times, it turns out that the government is much too busy watching for terrorists – that is, anyone from certain countries who is visiting on a visa or praying in a certain church – to spy on most citizens. It is actually much more difficult for a government agency to go through the red tape necessary to wiretap you (even after PATRIOT Act v1) than it is for private industry to include a request to bug your desktop in their EULA. If only George Orwell (*1984*) had known about PCs, it wouldn't have been the TV watching its viewers.