Privacy Watch: More Criminals Use Keystroke Loggers

By Andrew Brandt, PCW Print Nov 23, 2005 4:00 PM

Keystroke loggers--programs that secretly record every character you type--are getting much more common, security analysts say, as criminals use them to steal user names and passwords for financial and other accounts.

Websense, a computer security firm, reports that for stealing passwords many cyberpickpockets prefer keystroke loggers (keyloggers for short) to phishing. Unlike phishers, bad guys who use keyloggers don't have to create elaborate fake Web sites to trick people into divulging their bank passwords, for instance. Instead, the crooks just wait until the unsuspecting victim visits the real site. The keylogger records the keys the person types to log in and then it uploads the data to the criminals.

Websense says that the number of unique keylogger programs in use by criminals more than doubled between April 2005, when there were 77 of them, and July 2005, when the company saw 179.

Early in 2005 criminals used a keylogger to discover the password for accessing a computer that performs electronic money transfers at the Sumitomo Mitsui bank in London. Police learned of the plot to steal $420 million just before the bad guys could execute the transfer. Arcot Systems, which develops software used to thwart keylogging and phishing, says crimes involving stolen passwords result in $2.75 billion in losses each year.

To combat the threat, many online banks have started using software keyboards on their Web site log-in pages. Because you enter your password or PIN by clicking on-screen buttons rather than by typing the numbers or letters on your keyboard, this arrangement can defeat a simple keylogger. And because the Arcot software keyboard constantly changes the labels on its virtual keys, the bad guys can't tell what number you're clicking by recording the mouse pointer's location on screen every time you click.

Of course, crooks always counterattack. Some aim keyloggers at sites of financial institutions that don't use software PIN pads or other advanced security features. Others are beefing up their malware arsenal with software that can capture an image of your screen every time you click a number on an on-screen PIN pad.

Still, if you use a software firewall, keep your antivirus software up-to-date, and avoid running programs that you receive via e-mail or instant messaging, your chances of stopping a keylogger before it can harm you are good. The best way to determine whether a keylogger is running on your PC is to scan the system regularly with a good antispyware tool, such as Webroot Software's Spy Sweeper.

Andrew Brandt

Andrew Brandt is a senior associate editor for PC World. E-mail him at privacywatch@pcworld.com. To read previously published Privacy Watch columns, click here.

- See more like this:
- Privacy Watch,
- January 2006,
- January,
- keystroke logger,
- keystroke loggers,
- keystroke,
- logger,
- loggers,
- keyboard,
- character