



Protecting Your Organization's  
Critical Data From Keyloggers!

# Combating Keyloggers

*How to protect your company's computers against cyberspace's sneakiest attackers.*

Imagine there was a spy sitting inside your company's computer, recording everything your employees typed. This tiny undercover agent would diligently transcribe every single keystroke, creating strings of data reflecting financial transactions, business meetings, office memos and other crucial documents and activities. Every now and then the spy would silently transfer the collected information to a shadowy character located who knows where, who can then use the intelligence to steal funds, discover trade secrets, swipe employee identities and perhaps even undermine your enterprise's very existence.

This situation isn't as hypothetical as it sounds. According to telecommunications and security services provider Verizon, keyloggers and related spyware tools were a factor in 19 percent of all cases investigated by the company in 2009, responsible for 82 percent of all compromised records and making them most dangerous online security threat.

The problem is enormous. Even a casual Web search shows that keylogging software is abundantly available to anyone with even the slightest inclination to spy on computers used by other people. Simply typing the word "keylogger" into Google will return links to literally dozens of keylogger programs, many of which can be used by people with little or no technical knowledge or programming expertise. It's a scary situation, and one that's getting scarier each day.

## **What is a Keylogger?**

A keylogger is specifically designed to collect, monitor and log computer user actions. The code usually runs silently and unobserved in background, separate from everyday computer activities while silently recording all of the keystrokes a user makes. Keyloggers are typically used to collect user names and passwords, which can then be

used to access almost any type of private account. Most of these programs are run covertly to avoid tipping off users to the fact that their actions are being monitored.

Beyond basic key loggers are several other types of monitoring spyware, including such variations as:

**Screen Recorders:** These tools will capture anything that's displayed on its host computer's screen, such as account numbers, passwords, social security numbers and other types of confidential information.

**Chat Loggers:** This type of program captures keystrokes entered into a chat program. While generally more of a threat to consumers than businesses, a chat logger has the potential to hurt any organization that relies on chat clients for internal communication purposes or to connect with business partners.

**Email Redirectors:** Instead of capturing keystrokes or screen data, an email redirector takes a brute force approach to information piracy by re-routing incoming email to another computer. The capturing system then scans the text for potentially useful information.

### **Acquiring a Keylogger**

Like a cold or the flu, nobody actually seeks a keylogger infection. Instead, the code is typically picked up through a combination of user complacency and attacker deviousness. Keylogger files are often attached to downloads obtained from shady websites and emails. Once inside a computer, the attacker's code attaches itself to a commonly used program and then resides in the system's main memory where it works stealthily and efficiently, stealing and relaying user information. Sophisticated keyloggers are practically invisible on an infected machine, often running as a seemingly innocuous background process.

While most keyloggers are obtained inadvertently by mistake or neglect, the code can also be installed intentionally, such as by a disgruntled employee or an unethical competitor. In such cases, the code is usually installed with the help of a portable external storage device, such as a USB memory stick or portable hard drive. Employees can also inadvertently install a keylogger on their computer by bringing an infected portable storage device to work.

### **Detecting a Keylogger**

A big problem with keyloggers is that a great deal of intercepted data may have already been transferred before an infection is discovered. Unlike many other types of malware, which are designed to cripple or disable a computer—often in spectacular fashion—keyloggers' surreptitious nature often makes them difficult to detect by casual observation.

Poor system performance is often a tipoff to a keylogger infection. Since a keylogger resides and functions within a computer's main memory, the program can slow RAM performance. If a user is suddenly experiencing slower response times without having made any changes to the computer, chances are the machine is infected with some sort of spyware. Yet with computers becoming ever more powerful, it's becoming increasingly easier for keyloggers to operate without having any negative impact on system performance.

### **Getting Rid of a Keylogger**

Keylogger developers work hard to make sure that their creations can't be easily detected. This means that businesses with at-risk data need to seek the assistance of a powerful tool specifically designed to sniff out a keylogger in whatever form it takes and wherever it may lurk within a PC.

Most major anti-malware software vendors claim that their products have the ability to detect and neutralize keyloggers and related tools. Yet all-in-one anti-malware products generally do a poor job of rooting out spyware. The only certain way of detecting the full range of keyloggers and related spyware currently in circulation, as well as to eradicate or disable the code, is to use a product that has been designed 100 percent from the ground up to tackle the problem.

### **Why SpyReveal is the Answer?**

Detecting keyloggers is largely a numbers game. The problem with all-in-one anti-malware products is that they can only detect a limited number of keyloggers. While malware scanner vendors like to position themselves as steadfast guardians against all computer threats, they are in fact masters of none. In reality, most scanners fail to detect 70 percent of keyloggers available on the market.

SpyReveal, on the other hand, is to computer monitoring spy programs what a virus scanner is to viruses. Once downloaded and installed on your system, SpyReveal scans your entire system for the presence of any of the hundreds of computer monitoring surveillance spy programs available, far more than any competing product. SpyReveal achieves its efficiency because it isn't inflated with tools designed to fight adware, viruses, trojans or other kinds of malware already addressed by "all purpose" antivirus packages.

As you search for a solution to the keylogger threat, you also want a solution from a vendor that stands behind its software. SpyReveal backs its product a money-back guarantee. If, for whatever reason, you are not happy with SpyReveal within 15 days, the company will return your payment. Additionally, if your current anti-spyware software detects ANY commercial spy program that SpyReveal doesn't, we will give your money back.

## **The Bottom Line**

Your organization depends on its computers for an array of business-critical tasks. A keylogger infection will derail orderly daily tasks and throw your business into turmoil by exposing its critical financial and operational information to outsiders and by comprising the stability and reliability of enterprise PCs. This is a risk no business can afford, particularly when the cost of prevention is so minimal.

Since 1999, SpyReveal has had one basic mission: to detect commercial keyloggers and protect customers from surveillance software. SpyReveal runs on any Windows version from 2000 through Windows 7. While the software is 32-bit, care has been taken to ensure that it operates properly in 64 bit environments.

Take control of your company's computers and pull the plug on system spies by ordering SpyReveal today for a one-time fee of only \$49.95. Click here to get started:  
<http://www.spyreveal.com/>