Computer News

January 2006 - MTM Computer's Publication for Networking Solutions

Beware the Keylogger!!

A Key Logger is a program that runs in the background, recording all keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system.

A Key Logger normally consists of two files: a DLL which does all the work and an EXE which loads the DLL and sets the hook. Some of these programs come with an additional installer program that re-installs the Key Logger if some utility tries to remove it from the system.

Some Key Logger programs also come with an option to capture screen images. Still other programs have the ability to secretly turn on video or audio recorders, and transmit what they capture over your internet connection. These are some of the things these programs can do:

- Internet Conversation Logging – Log both sides of all chat conversations for AOL/ICQ/MSN/AIM Instant Messengers, and view them in real time, as they are happening.
- Window Activity Logging – Capture information on every window interacted with.
- Application Activity Logging – Track every application/executable that was executed and interacted with.
- Clipboard Activity Logging – Capture every text and image item that was sent to the clipboard on the remote machine.
- Keystroke Monitoring – Track all keystrokes and pressed keys and which windows they were pressed in. Keystrokes can also be passed through a formatter for easy viewing/exporting.
- Websites Activity Logging – Log all websites that were accessed on the remote machine.

Information captured by a Key Logger can be sent back to the malicious user via the Internet directly to a website using File Transfer Protocol (FTP) or via e-mail. This e-mail does NOT show up in your “Sent List”.

Key Loggers can be installed on your system without your knowledge. They can be installed just by visiting a website. Someone can e-mail you an advertisement for some product or service with a link to their website for more information. When you click on the link and visit their website, the Key Logger is installed while you are looking at the pictures or reading the ad. Key Loggers can be attached to other programs and installed when you install the other program. For example, you can attach a Key Logger program to a “Freeware” program and e-mail this to someone. When that someone opens up that e-mail attachment to install the free program you sent them, they get the Key Logger program installed also, totally without their knowledge. Examples of these “Freeware” programs are Waterfall screensavers, MP3 players, even programs like Spybot Search & Destroy! The host program can be a legitimate freeware tool but it comes with a hidden package that you never see. This is where the name Trojan comes from. It refers to the Trojan Horse where soldiers where hidden inside a gift.

How do you avoid Key Loggers? Well there are several different approaches. Key Loggers are part of a family of software called Spyware. You can use utilities like KeyPatrol, PestPatrol, PPMemCheck, CounterSpy, Microsoft Antispyware, Ad-Aware and Spy Sweeper to detect and remove Key Loggers and other types of Spyware. The essence of any Spyware prevention exercise is first to ensure the operating system is fully patched to known vulnerabilities. The best prevention is to educate users that it is not safe to click on anything and everything found on the Web, and they must also install only what is needed. Freebies on the Internet, ones which are often typically advertised in pop-up banners, must be totally abstained from. Other methods of avoiding Spyware are to ensure that the browser you use is configured securely, and to have at least one good Spyware detection and removal tool installed. You can try using a less popular browser hoping that the bad guys have left it alone, but as soon as people start to move to a new browser and it catches the eyes of attackers, it is only a matter of time before this new browser gets hacked. Firefox was the browser to use to avoid security hacks until it became popular, now it has more vulnerabilities than Internet Explorer.

Con't on next page...

Computer News Con't.

Keylogger's Con't.

One thing you can do to be safe when entering sensitive information on your computer is to use a Virtual Keyboard. A Virtual Keyboard is analogous to a graphical keypad where a user clicks on the characters rather than types them on the keyboard. This approach may not be practical for every user; however, it can be still be useful for very sensitive applications. Note however that even this approach is not completely secure, as some Key Loggers are designed to capture screenshots on every mouse-click. Thus, the password of the user can still be found out when a virtual keyboard is used by looking at the screenshots. To avoid this, some virtual keyboards also have a feature that allows a user to enter a character by hovering the mouse cursor over a letter for a few seconds. Thus the user can enter the password without even clicking the mouse button.

There is Anti-keylogging software available from various vendors. This software can identify known key loggers if they are found on your system with varying degrees of success. Key Loggers that have the feature of renaming themselves however will not be detected by "signature based" Anti-keyloggers. "Hook based" Anti-keyloggers use a process that many of the Key Logging software programs use themselves which prevents the Key Logging software from working. The "Hook based" programs generally work better than "signature based" Anti-keyloggers; however, if the Key Logging software loads at the kernel level, they will be loaded before the Anti-keylogging software can be installed which means the Anti-keylogging software will be ineffective.

With the vast proliferation of Spyware in recent years, there has been a growing list of websites and malicious users trying to cash in by installing Key Loggers and stealing personal information. Identity theft has become rampant. The need of the hour is to be aware of such common practices in Spyware, and recognize it for what it is: malicious code that should always be avoided.

Be Safe out there !!

Q :
Help! My computer just started making a strange sound when I turn it on. It sounds like rapid ticking or rattling (not hard drive sounds either) and goes away after a few minutes. Any ideas?

A :
Sounds like a problem with one of your fans. No, not the people who love you, the machines that blow air.

Your computer probably has two internal fans. One sits on top of the CPU, and one is inside your power supply. The sound you're describing usually comes from the fan in the power supply. They can make that annoying noise for a long time before they finally belly up and die. However, if it's your CPU fan, you may have a serious issue. If that puppy dies, your CPU can turn to toast in a hurry. Trust me, they're not very good with butter and jelly!

The best advice is to wait till your computer is completely cooled off and remove the case cover. Turn the computer on and see if you can determine where the sound is coming from. If it's the CPU fan, that will need to be replaced. If it's the power supply fan, you'll need to replace the entire power supply to get rid of the noise. Don't think you're going to open the power supply and fix the fan. They're not user serviceable and if you touch one of its capacitors by accident, you'll take a nice little flight across the room. Remember, these power supply fans can work for years after they start rattling, so usually there's no rush. That doesn't mean you shouldn't keep a close eye on it, though. If that fan dies, your computer can overheat in a hurry.

You may want to listen to your hard drive, too. It's the square, slim box. The sound described in the question above probably isn't hard drive-related, but it's always a good idea to give it a quick listen.

After you're done playing with your machine's innards, be sure to put the cover back on. Believe it or not, your computer can overheat with the cover off. The computer is designed to pull air through the case in a certain pattern. If there's no cover, the airflow goes all wrong, and things won't cool as they should.

Happy New Year,
May you all have a Healthy, Happy & Prosperous New Year !!

MTM Computer Consulting, Inc. 805.583.5585 e-mail: Sharon@mtmii.com