Keylogger

Keylogger

Keylogger is a device or program that captures every keystroke made on a computer via a keyboard. An intruder can make use of keylogger to record and monitor all keystrokes entered from a user's keyboard remotely so that personal information such as credit card number, username and password can be captured. Therefore, a keylogger is also considered as a type of malicious code like spyware, which can steal information. Attackers may use keylogger together with other malicious code to launch their attacks.

Causes of Infection

The attack method of keylogger is very similar to that of a computer virus. The chance for your computer of being attacked may be increased if you have done the following:

- Install or open files or software from unknown sources;
- Open emails from unknown sources and their attachments;
- Visit malicious websites such as fraudulent websites.

Potential Threats

By capturing and monitoring the data input from keyboard, intruders could gather valuable information especially account numbers and passwords from users. The intruder may impersonate the legitimate user to perform illegal activities. For example:

- Log on the user's online banking account, change user's password, steal money from the account or perform illegal transactions through the account.
- Log on the user's email account, change the user's password and send spam emails and propagate computer virus.
- Log on the user's system which has been previously visited by a user, to

steal internal information from the system e.g. name of clients and credit card numbers etc.

General Security Precautions

To effectively prevent your computer from being installed with a keylogger, you should pay attention to every online security measures in your daily use of computer. For example:

- Avoid performing any sensitive operations such as Internet banking in public computers.
- Do not visit suspicious or untrusted websites, or download programs and software from them.
- Do not open emails or their attachments from an unknown source.
- Use 2-factor authentication for online services or systems, such as smart card plus password.
- Scan electronic portable devices with anti-virus software before using them.

Furthermore, you must apply basic security measures on your computer, including installing anti-malicious code software (such as anti-virus software), firewall and latest security patches, scheduling a weekly full scan and enabling the Auto Update feature of relevant software.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk