What is a keylogger?

What is keylogger? Many people may vaguely understand that keyloggers are something dangerous that can record every keystroke, but not everyone knows about the tool.

What is keylogger? Many people may vaguely understand that keyloggers are something dangerous that can record every keystroke, but not everyone knows about the tool.

Certainly, in us, many people are not less than 1 time listening to the concept of 'keylogger'. Although it can be felt vaguely that it is dangerous, a powerful tool can help bad guys steal information that we enter from the keyboard. But can you confidently say that you fully understand this tool? Join us in learning about the keylogger, its purpose, the type of information it gathers as well as the way it works, thereby drawing the most effective protection experiences.

Main content about keylogger in lesson

What is keylogger?

Keylogger is usually a small software - or sometimes more dangerous, even a hardware device - with the ability to **record every keystroke the user has pressed on the keyboard** . Combining the results of these keystrokes, keylogger installers can obtain personal messages, email content, credit card numbers and of course the most dangerous is all kinds of user passwords.

What is the keylogger used for?

Keylogger is used in Information Technology (IT) organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used by a family (or business) to silently monitor members' network usage; sometimes they are used as part of child monitoring.

The last and most dangerous purpose of keyloggers is that hackers, dark conspirators can install keyloggers on computers to steal passwords, personal information, secrets or credit card information. .

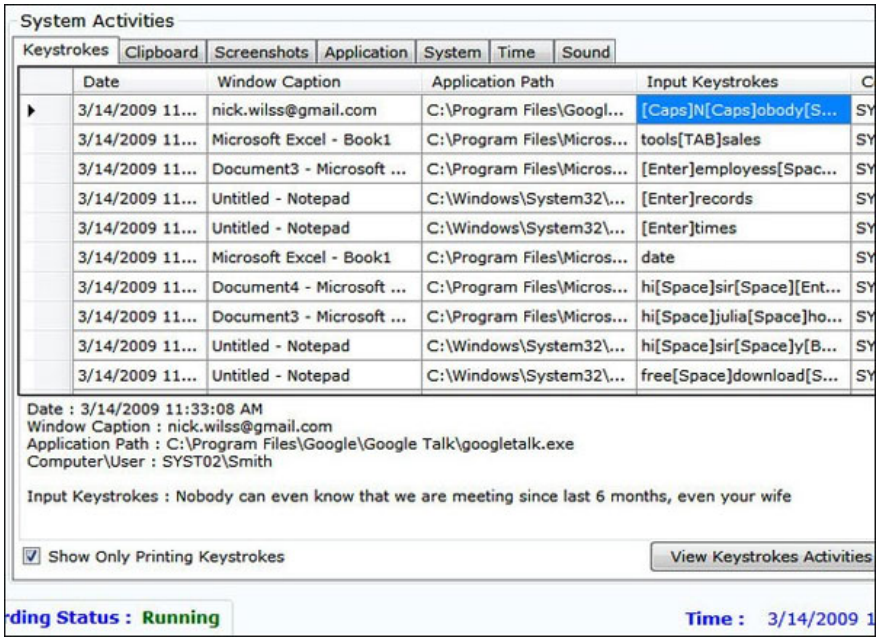
What keylogger information can collect?

Depending on the type of keylogger and the purpose of the creator it has different capabilities, but when mounted on the device, it can often perform the following actions:

1. Record any password entered by the user on the device.
2. Take a screenshot of the device according to a certain cycle.
3. When re-entering the URLs the user has entered with the browser, even take a picture of the web pages the user has viewed.
4. Record the list of user applications running on the device.
5. Capture recordings of all instant messages (Zalo, Facebook Messenger, Skype, Viber, .)
6. Capture copy of sent email
7. Automatically send reports containing stored logs and send email to a remote location via email, FTP, HTTP.

Most keyloggers not only record user keystrokes but also capture computer screens. Keylogger can store the data it collects right on the user's hard drive or automatically transfer data over the network to a remote computer or Web Server.

How does the keylogger get into the machine?



In most cases, the keylogger is **silently installed by malware on the user's computer** after successful penetration. Some other cases are somewhat less common when parents want to manage their children's access, when managers of a company want to check their work attitude or… couples want to follow each other . In Vietnam, sometimes we hear that keyloggers are in net-order machines - not because of a machine infected with malware but by someone who wants to 'try out his skills', even someone even gives that it is the owners who

direct this. The reality of the rumors as well as the legitimacy of the cases touches on the privacy of each person - even if the parents want to monitor their children is still within controversy. But the need to manage employees of large organizations through keyloggers is real, and people even have specialized hardware product lines for this job.

As mentioned above, most keyloggers on common computers are distributed through malware. If the user's computer has been compromised, the malicious code may have the function of a small keylogger software - or it can act as a Trojan, proceed to download and install the keylogger package. silently, even with many other malicious software. Often malware will also automatically set up a channel to send the keylogger information to the 'owner'. It can be said that keyloggers are one of the most popular hackers because they can capture all kinds of user information using this method.

In addition to the malware infiltration channel, most of the remaining keylogger infections come from our relatives. The two subjects are most relevant, as stated before, of course, parents and . lovers (or spouses). Parents feel the need to control the amount of access to their child's vast Internet world often using parental controls, which are often not difficult to find similar functions to keyloggers. . And of course in today's cyber world, a jealous girl with a bit of English will only take less than 30 minutes to get Google to install a keylogger (or even more multifunctional software) to track See if you sneakily "eat pho" outside.

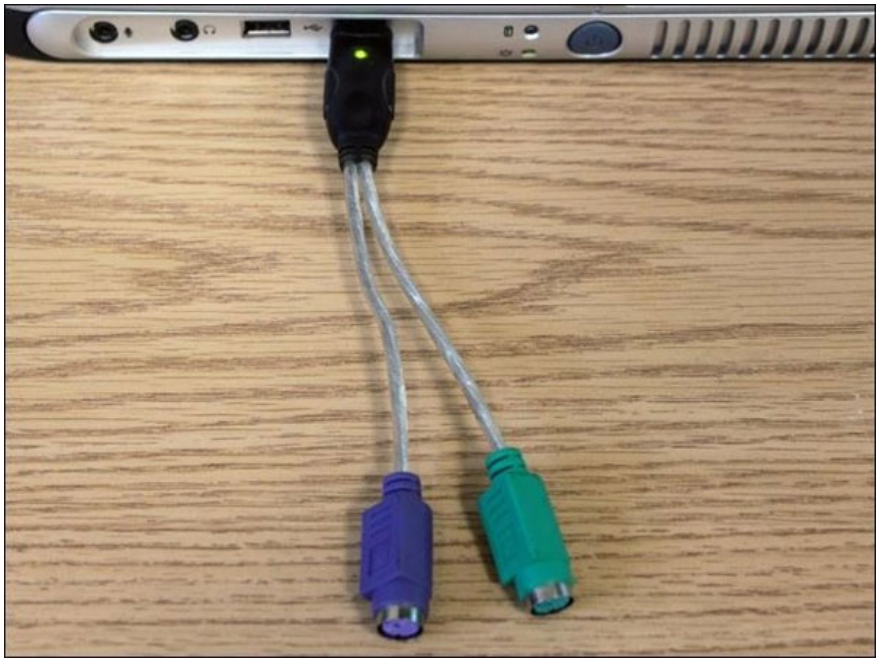
In case the boss directs the installation of keylogger on the employee's machine , remember that analyzing the results of keylogger, especially with a large number of machines, is not a waste of effort and resources. . In most cases, if you find yourself in 'focus', check yourself to see if you have anything to do with being a 'suspect object' to reveal the company's information first. The laws related to this tracking issue also vary depending on the country and geographic region. At the same time, some companies also require employees not to work personally in the workplace environment, so such monitoring is still considered by some to be legal and reasonable - because if you enter information anyway. Individuals on these machines mean that the employee himself has violated the rules, cannot blame anyone else.

Keylogger software

These are keyloggers configured in programs that run on your computer. These keyloggers are installed on your computer by hackers and run in the background, in some cases users can hardly detect.

This type of keylogger is used to forward data to hackers. They can 'paralyze' your system.

Hardware keylogger



With the advancement of technology today, creating a keylogger as a hardware device is no longer too difficult. As we all know, PC keyboards are usually connected to the case via a USB cable (or some models still use the PS2 port). Connecting specialized hardware keyloggers simply disconnects the keyboard to the case, plugs into a compact keylogger device. This device of course is then connected to the case to ensure that users can still enter the data normally without any detection, especially in some business environments where the case is normally closed. closed and sometimes only IT staff have access keys. Even in the net shop, or with careless users who never touch the dusty case under their tables, this way is still very effective. With this method, no security software installed on the machine can help us discover that the data entered from the keyboard is silently recorded, because this device does not inform the operating system. act on its presence.

While often not as advantageous as malware-installed software, it is possible to send data obtained over the network. But the person who installs the keylogger device only needs to go back a few days, unplugging the device and plugging the keyboard back into the old one has a relatively large amount of data on the user's hands. The most important thing is that it does not leave any "soft" traces to the eyes of security software, connection analysis . can be discovered.

Sometimes, these devices can also be disguised as adapters that look very 'gentle' as shown in the picture above. Or appear in USB or other portable hard drive devices. In most cases, these keyloggers are embedded on the back of the CPU to record the user's keystrokes.

How the keylogger works

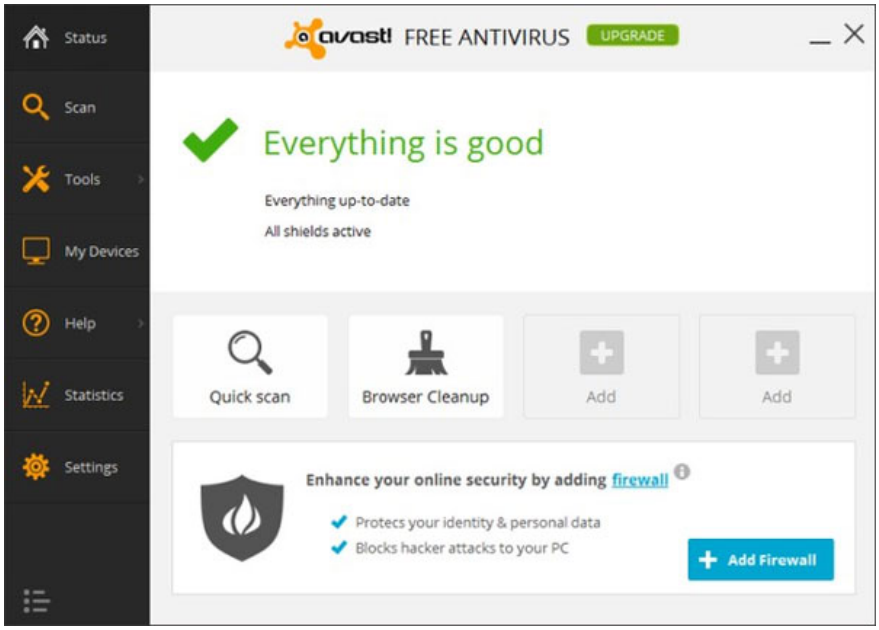
Keylogger in the form of software often runs in the background, recording every keystroke the user enters. Sometimes to avoid sending data regularly that keeps track of users 'attention', these software packages can be designed to only send seemingly useful data strings - such as a string numbers 'seem' like credit card codes.

To increase efficiency, keyloggers are often combined with other types of tracking software, so intruders can distinguish the information that users enter when meaningless chats with input information. when you are logged in to your online bank account. The first string of characters users enter after starting a **chat program, email client or online game is also important** - because this is usually the username and password used to log into

that service account.

In cases where it is necessary to be more 'cared for', the keylogger installer will often have to use the tool to scan through the entire log file to record all the user has entered during the time being followed. From there, it will filter out all kinds of information, such as the content of Google search, comments in a topic, etc., online. Often the tracking software package provided for parents and offices also includes screen capture utility. From there provide sufficient information and evidence of what the 'victim' did during the process of using the device.

Protect yourself against keyloggers



At the core, the keylogger software has always been classified as malicious code - malware. So we can detect keyloggers on the computer using the most commonly used scanning tools. Most importantly, choose the right security software - no need to be strong and expensive, just have a name and a clear reputation. Avast, AVG, Avira all have free and effective solutions for general users. If not careful, it is possible that the software that assigns 'anti-virus' or 'anti-malware' that you download from a certain source on the network is the culprit of installing keylogger on your computer, or more gently. it will entail countless bloatware - unwanted software - as well as annoying ads on the device.

If you are really worried and unsure about the existence of a keylogger or further is the management software installed by others on your computer, it is always best to take advantage of the virtual keyboard function available on the service. banking services, online payment channels or online games. Do not let a beautiful day after logging in to the game, troubled to recognize that his character has been "stripped naked", while the culprit is not strange but is the level . parents.

See also: Instructions for finding and deleting the original Keylogger from your computer

You finished reading the article "**What is a keylogger?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com