# Keyloggers: A Threat to Your Data

Ezequiel Guerra

East Carolina University

ICTN - 4040

Instructor Dr. Peng Li

As more and more people throughout the world utilize the Internet to access their personal data. The greater the chance their data can be stolen. Millions of people access a variety of online accounts and websites daily such as email, banking, shopping, stock market, billing, career and social media. In this paper, I will be discussing a major threat to your data and accounts, keyloggers.

A keylogger, (which is short for keystroke logger) is essentially as the name implies. It is a device or program that monitors and logs the keystrokes that a user types on a keyboard. The data that's collected by the keylogger can then be retrieved at some point in the future, either physically or remotely. Some modern keyloggers have additional features that allow you to do more than just log keystrokes. There are two main types of keyloggers that I will be discussing, hardware and software.

Hardware keyloggers are hardware devices that record your keystrokes; they generally contain a micro-controller and internal memory, usually flash memory. The micro-controller interprets the data from the keyboard, processes it and sends it to the internal memory for storage. Hardware keyloggers are usually connected in-between the keyboard cable connector and computer connection. There are some keyboards available that have hardware keyloggers already built-in to the keyboard however, these are less commonly used. The most common hardware keyloggers are USB inline devices. There are also USB wireless versions for wireless keyboards and PS/2 versions for older keyboard connectors. These types of hardware keyloggers can be installed quickly, easily and can store several gigabytes of data and are relatively inexpensive. Some examples of USB and PS/2 keyloggers are shown below in Figure 1.


***Figure 1: USB, PS2 Hardware Keyloggers***

As you can see hardware keyloggers tend to look like legitimate adapters and may not be recognized as a keylogger by someone who notices one. Hardware keyloggers are simple to use and can even be used by the most novice computer user. Once a hardware keylogger is plugged in, it will start recording keystrokes from the keyboard as soon as the computer is turned on. This allows your login and/or password for your operating system to be captured, it would also be able to capture your BIOS password if your system is equipped with one. After a keylogger has been recovered from its victim it is easy to retrieve the data that was collected. Generally, all that is needed to retrieve the data from the keylogger is to simply open a text editor like Notepad and type in the password given by the manufacturer or one that was previously set by the attacker.

The hardware keylogger will recognize the password and open a menu with options that allow you to choose what it needs to do next. Some of the options you may see on the menu would allow you to download the data in memory, erase the memory, run diagnostics, upgrade the firmware and change the password to the keylogger. Because a hardware keylogger works by capturing signals from the keyboard at the hardware level they cannot be detected by software programs. A visual inspection of your keyboard connection is the easiest way to check if you have a hardware keylogger on your system. If you find a hardware keylogger on your system,

you can just physically remove it from your computer system to keep it from capturing anymore data. An example of a keylogger menu is shown below in Figure 2.

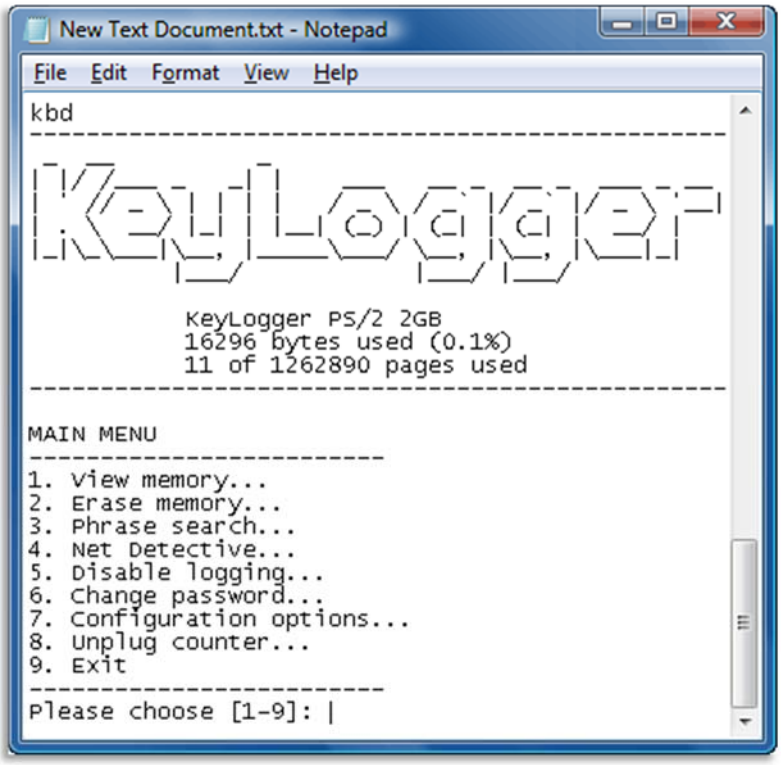


***Figure 2: Hardware Keylogger Menu***

Before I get into the topic of software keyloggers, let's discuss some of the reasons keyloggers are used. Keep in mind that the reasons can be ethical or unethical depending on the intent of the person using the keylogger. Keyloggers may be used by parents who want to monitor their children's computer activities to make sure they aren't getting into something they shouldn't be. Law enforcement could utilize a keylogger to obtain evidence to investigate theft or espionage cases. Businesses sometimes use a keylogger to monitor their employees to make sure they are using work resources for business purposes only. A hacker or a person with malicious intent may use a keylogger to steal logins, passwords, credit card data, identity information or to capture other important data the target may have. In some cases, keyloggers are

used by a husband or wife to get proof of adultery if they suspect that their spouse may be cheating. Before using a keylogger it's a good idea to check with local laws to make sure that what you are capturing is legal.

Software keyloggers have more features than a hardware keylogger because they work with your computers operating system. In most cases software keyloggers are packaged with backdoor programs and installed via malware. A user may accidently install one by opening an email attachment, visiting a website that's infected, thru social media, over point-to-point networks or EXE files that a user downloads. They may also be installed directly by a person who has access to your computer. There are several different categories that software keyloggers use to embed themselves in your computer system. Some of the main categories are: hypervisor-based, kernel-based, API-based, form grabbing based, JavaScript-based, memory injection based and remote access based.

- **Hypervisor-based** - Using this method the keylogger can in theory exist outside the operating system and be treated as if it were a virtual machine.
- **Kernel-based** – This method obtains root access on your computer via a rootkit to hide itself inside the operating system. It then intercepts your keystrokes that pass through the kernel. Because the keylogger exists at the kernel level it makes this type of keylogger very difficult to detect.
- **API (Application Programming Interface) based** – This method is applied by hooking the keyboard API's inside a running application. The keylogger will register keystroke events just as if it were a normal part of the application. This is the most common method used to implement a keylogger.

- **Form grabbing based** – This method logs a user's web form submissions. Whenever the user completes an online form in a web browser and submits it by clicking ok, submit or enter. The keylogger recognizes it as a submit event and records the form data before it is sent over the Internet.
- **JavaScript-based** – This method injects a script tag into the targeted web page and listens for key events. Scripts are injected by using different methods, including cross-site scripting and a man-in-the-middle attack.
- **Memory injection based** – This method logs the data by changing the memory tables that are associated with system functions and/or the web browser. This method can be used to bypass Windows UAC (User Account Control) by patching or injecting directly into the memory tables.
- **Remote access based** – This is a feature that is added to some keyloggers, it will allow access to your locally recorded data from a remote location. The recorded data can then be emailed, uploaded to a database, FTP server or website to the person that has access to the keylogger.

Software keyloggers can hide in hidden directories, disguise themselves as legitimate operating systems files or hide themselves from the operating systems task manager by using some of the techniques in the categories listed above. They can be very difficult to detect because they are programmed to hide their presence.

To detect and remove a software keylogger an antivirus and/or anti-spyware program like Avast, AVG, Norton, McAfee, Malwarebytes or Spybot Search and Destroy can be used. Most antivirus and antispyware programs use a signature from a database to detect keyloggers so, it is important to keep antivirus protection up to date. If you suspect that your computer is infected

with a keylogger and the antivirus or anti-spyware scan comes up clean. There are programs called anti-keyloggers that can be used. These programs are specifically designed to detect and remove keyloggers. Like antivirus software anti-keyloggers also use signatures from databases, however, they are strictly focused on keylogger signatures. Anti-keyloggers also utilize heuristic analysis, meaning that they look for known features, attributes, or methods that keyloggers have been known to use. They are also capable of detecting hidden unassembled keyloggers that are in the computer system. SpyShelter and Zemana are two popular anti-keylogger software programs.

Software keyloggers are mainly viewed as a threat to computers because of their physical keyboard use. This may lead you to believe that smartphones are safe from keyloggers because of their touchscreens. At one time this was true, keyloggers were not a viable threat to smartphones with touchscreens, however, this is no longer the case. Over the last few years' smartphone sensing capabilities have gotten much more precise. Researchers have been exploring new attacks that exploit the built-in motion sensors in smartphones to deduce the users taps on the smartphones touchscreen.

In an article titled, "The Rise of Keyloggers on Smartphones" in the *Pervasive and Mobile Computing Journal*. It referenced studies conducted on a couple of software programs called, Taplogger and Touchlogger. These two programs use a smartphones multiple sensors to log the X-Y and/or Z coordinates of the smartphones touchscreen to help log the tapped keystrokes. Although accuracy and ease of installation currently varies with these programs, the studies show that in the future keyloggers will become much more of a threat to smartphones.

Keyloggers can be a major threat to your data. They could allow someone to collect information about you and then use that information to steal your identity and access your online

accounts. The information captured by a keylogger can vary depending on the type of hardware or software keylogger used. Some common items captured by keyloggers:

- Any keystrokes that you enter on your keyboard
- BIOS passwords
- Screenshots (can be taken at regular intervals)
- Items that have been copied to the clipboard
- URL's that a user visits thru their web browser
- Applications that a user is running
- Instant messaging conversations
- Copies of sent emails
- Documents that are sent to your local printer
- Sound and video (if you have a camera and microphone attached)

An example of items captured by a software keylogger is shown below, in Figure 3.

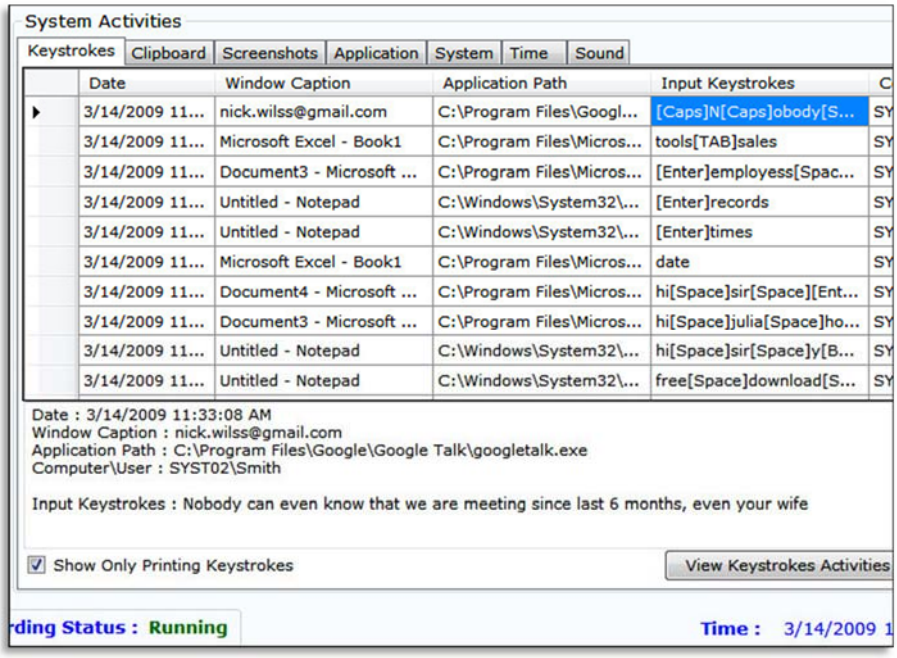


***Figure 3: Items captured by a software keylogger***

The following is an example of the kind of damage a keylogger can do if you aren't proactive in protecting your computer system. In February 2005, a Miami, Florida businessman named, Joe Lopez, filed a lawsuit in Miami Circuit Court against Bank of America. He filed the lawsuit after $90,348 had been stolen from his bank account via a wire transfer to Latvia. Mr. Lopez filed the lawsuit claiming that Bank of America was negligent in protecting his bank account. After an investigation, it was found that Mr. Lopez's computer was infected with a backdoor program called Coreflood, which contained a keylogger.

The keylogger recorded all of Mr. Lopez's keystrokes which included his bank account information and the captured data was sent to the hackers via the internet. This allowed the hackers to gain access to his Bank of America account and transfer the money to Latvia. In 2003 almost all antivirus programs contained the signatures needed in their databases to remove Coreflood. Unfortunately, Mr. Lopez had failed to take the basic necessary steps to secure his computer system with up to date virus protection. Since it was not Bank of America's responsibility to ensure that Mr. Lopez's computer systems were secure and protected. The court ruled in favor of Bank of America and Mr. Lopez was not able to recover his losses.

In conversation, most people tend to hear about phishing schemes, ransomware, adware, URL redirects, viruses or spyware. It's not often that you hear about keyloggers, unless you are conversing with someone in the Information Technology field. It's important to keep keyloggers in mind as they can be extremely dangerous. Hardware or software keyloggers can be installed very quickly. If you leave your computer unattended or aren't careful with the attachments, programs, downloads or files you open your data can be stolen in a matter of minutes. It's good practice to keep your computer password protected, have up to date antivirus software and it is not a bad idea to periodically check your keyboard connection for a keylogger.

## References


Grebennikov on March 29, 2007. 1:03 pm, Nikolay. "Keyloggers: How they work and how to detect them (Part 1)." *Securelist - Information about Viruses, Hackers and Spam*. N.p., 29 Mar. 2007. Web. 08 Apr. 2017. <https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/>.

Hardware Keylogger Photos. Digital image. *Keelog*. N.p., 09 Mar. 2017. Web. 8 Apr. 2017. <https://www.keelog.com/wifi_hardware_keylogger.html>.

Hoffman, Chris. "Keyloggers Explained: What You Need to Know." *How To Geek RSS*. N.p., 27 Jan. 2014. Web. 8 Apr. 2017. <https://www.howtogeek.com/180615/keyloggers-explained-what-you-need-to-know/>.

Hussain, Muzammil, et al. "The Rise of Keyloggers on Smartphones: A Survey and Insight into Motion-Based Tap Inference Attacks." Pervasive and Mobile Computing, vol. 25, 2016, pp. 1-25, doi:10.1016/j.pmcj.2015.12.001.

Mitchell, Bradley. "Why keylogger software should be on your personal radar." *Lifewire*. N.p., 18 Oct. 2016. Web. 8 Apr. 2017. <https://www.lifewire.com/definition-of-keylogger-817998>.

Pathak, N., Apurva Pawar, and Balaji Patil. "A Survey on Keylogger: A Malicious Attack." *International Journal of Advanced Research in Computer Engineering and Technology* (2015). *

Siciliano, Robert. "What is a Keylogger?" *McAfee Blogs*. N.p., 28 Oct. 2016. Web. 8 Apr. 2017. <https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-a-keylogger/>.

Smith, Donald. "Customer vs. Bank of America: Who's to blame?" *SearchFinancialSecurity*. N.p., 17 Jan. 2008. Web. 08 Apr. 2017. <http://searchfinancialsecurity.techtarget.com/news/1294508/Customer-vs-Bank-of-America-Whos-to-blame>.

Tuli, Preeti, and Priyanka Sahu. "System monitoring and security using keylogger." *International Journal of Computer Science and Mobile Computing* 2.3 (2013): 106-111. *

Wood, Christopher, and Rajendra Raj. "Keyloggers in Cybersecurity Education." *Security and Management*. 2010.