What is a keylogger?

A keystroke logger or a keylogger is generally a software installed on the computer which is designed to record all keystrokes made by the user. Some examples of software keyloggers include EasySpy, KidLogger and BlackBox Express. Other types of keyloggers can be found in the form of hardware such as the KeyGrabber USB keylogger, but still perform the main similar functionality of logging keystrokes.

What are some features of keyloggers?

Besides recording key presses from the keyboard, advanced software keyloggers can be extended with a number of other recording-typed features that may include a diverse range of inputs. These may include but are not limited to:

- Clipboard logging - recording what and when the user copies to the clipboard.
- Screen logging - capturing screenshots of part or whole of the user's screen. An example of the use of this feature may be to capture screenshots of the user's computer screen when their mouse is pressed to overcome the security of virtual keyboards offered by the websites of some banks.
- Audio recording - recording audio of the user such as their keystrokes via hijacking the user's computer mic.

What are the uses of a keylogger and their application throughout history?

Keystroke loggers are normally used with the intention of the person typing the keyboard being unaware that their keystrokes are monitored. Keystroke loggers can be used intentionally for legal activities such as parental monitoring, and scientific research on language and writing. One popular and perhaps illegal use (depending on the situation), is to monitor and investigate device activity suspected of inappropriate activity such as the activity of a romantic partner or a criminal suspect. However, keyloggers can also be used with the malicious intent to steal sensitive or personal information such as passwords, bank account details, search history and emails.

During the early introduction of keyloggers, during the 1970s up until 1984, the Soviet Union installed the hardware keylogger named as the 'selectric bug' into IBM typewriters to spy activity on U.S. diplomats in the U.S. Embassy and Consulate buildings in parts of Moscow and St. Petersburg. Keystrokes were captured via measuring the magnetic field emitted from the movement of the typewriter's printhead. On the other hand, the Russians protected themselves against any keylogging activity by opting for manual typewriters.

From the 1990s and onwards, there has been an increase in keyloggers created with the intention of serving as malware and occasionally used alongside phishing activities. The use of software based keyloggers at the time was popular as it was easier to imbed the keylogger into a system without having to install hardware into the user's computer. To the public, keyloggers

have often been commercialised heavily particularly towards concerned spouses or parents to monitor home computer activities and IT companies maintaining data loss prevention (DLP) protocols. In large companies, keyloggers have been used to check that employees are working appropriately on company computers.

Keyloggers have also been used in police investigations to track down criminal activity. For instance, in January 1999, the FBI embedded the keylogger, FlashCrest iSpy, into Nicodemo Scarfo, Jr. 's computer for charges against illegal gambling and loan-sharking after obtaining a search warrant. In doing so, the FBI was able to obtain the PGP (Pretty Good Privacy) passphrase (password) on his computer which allowed them bypass the PGP encryption program on Nicodemo's computer and obtain access to his encrypted illegal business records and other personal files.

How do keyloggers work?

Keyloggers are able to run hidden in the background. Depending on the keylogger, keylogging can work in several different ways. One way is that certain actions such as mouse clicks can trigger certain recording capabilities within the keylogger.

For most hardware keyloggers, when the user types on the keyboard, the keylogger records and stores the keystrokes as text onto its own hard drive. Wireless keyloggers on the other hand function by intercepting the communication between a wireless keyboard and the computer then wireless transmitting the data via its hardware system.

On the other hand, software keyloggers may log files and send the log files to a user via email, become stored in the computer or upload the data into a website, database or FTP (File Transfer Protocol) server.

On mobile devices, since modern day phones do not require a keyboard to type, normally these keyloggers log keys by listening to key sounds and translating specific sounds to a different key on your screen keyboard. Moreover, by gaining access to the phone's camera, microphone and networks, other personal information other than keystrokes can be logged.

How does one's computer get infected by a keylogger?
A keylogger can be installed via clicking on a dangerous link such as one that opens up a website which installs the keylogger onto your computer.

Inside the computer, a keylogger can be located in one of many places such as the operating system of your computer, the memory space used by programs or they can act as a driver on your computer. For example, a kernel driver keylogger can inject itself into the operating system by performing the similar functionality of the operating system to interpreting keystrokes.

For keyloggers in the form of hardware, given physical access to the target's computer, these devices generally are required to connect a USB (refer to figure 1) or P2/2 (refer to figure 2) port to function or have the device already inbuilt within the keyboard.

Figure 1. Hardware USB Keylogger

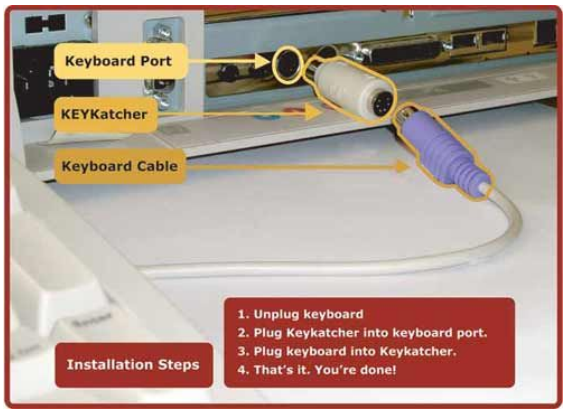

Figure 2. Hardware P2/2 Keylogger

Currently, there are no hardware keyloggers known to infect mobile devices. However, software keyloggers can infect mobiles devices.

How do you detect keyloggers?

Some signs of easily detected keyloggers to look for on your computer can be but are not limited to:

- Finding a foreign icon on your taskbar
- Finding a notification about the keylogger being installed in your notifications tray
- When you are experiencing an obvious delay when typing on the keyboard or when using your mouse.
- When you receive an error message when loading webpages.
- Finding an unknown hardware device connected to the back of your pc at the USB or P2/2 ports

On mobile phones, some obvious signs may include:

- When the phone is overheating after all apps and programs have been closed
- When the phone battery is draining quickly when device usage has been low
- When your phone receives suspicious text messages
- When there are strange noises originating from your phone. This may signal that the keylogger may be eavesdropping.

On the other hand, not all keyloggers can be easily detected and in fact can be very challenging to find. For example, a keylogger called the KeyGrabber module, works by manually being embedded within a keyboard and information can be received wirelessly via a transmitter or by manually removing the module from the keyboard before extracting the data it has collected.

Other keyloggers may be able to inspect the connection to your computer and your wireless keyboard to log the keystrokes from there.

Moreover, there exists software such as KL-Detector or MalwareBytes which can be downloaded to detect keylogging activity for you. These sorts of software may not detect all kinds of keyloggers but provides you a basis for detecting a portion of keyloggers that may infect your computer.

Another method is to examine any unknown or suspicious programs running on your task manager and use your system configuration utility to view programs loaded on start up.

What are some ways of protecting yourself from keyloggers and deleting/removing keyloggers from your device?

There are many ways to protect yourself from software keyloggers including:

- Using a software keyboard when logging into accounts - this method would only be effective against keyloggers that are only triggered by keyboard input and do not take screenshots.
- Using some sort of speech to text software to remove any keyboard input- Like the first point, this method is only effective against keyloggers that are only triggered by keyboard input and do not track microphone activity.
- Having an anti-virus or anti-keylogger program/app installed on your device - Anti-virus program such as Trend Micro can scan and detect some keyloggers as malware, block these programs from running and even sometimes remove these keyloggers. Anti-keyloggers such as Ghostpress prevent your keystrokes from being recorded by malware and may even prevent screenshots from being taken.
- Setting up a firewall - this may detect and block any transmission of data between the target and the attacker
- Using password managers which automatically fill in usernames and passwords - this will prevent triggering the keylogger via keystrokes.
- Install anti-screen capture software to prevent any keyloggers taking screenshots of your device
- Ensure all software applications and your operating system are up to date to replace and remove any old versions which may have a keylogger infected inside.
- Inspect the processes listed on your task manager and scan through for any suspicious programs you cannot distinguish. Uninstall any programs identified you have identified as suspicious to remove the keylogger. On Windows, this can be performed via the control panel.

For hardware keyloggers, the following ways may protect you:

- Perform spot checks on the computer that you are using. These may include devices connected to USB ports or P2/2 ports. If there are any suspicious hardware connected to these ports, remove them as these may be keyloggers.

- Purposefully type sensitive information out of order. For example, type the last letter of your password and move your cursor back to type the first letter of your password. This is known as deceptive typing.
- Replace your keyboard if you suspect it has been tampered with.

Other ways to protect yourself from keyloggers is to perform basic preventive cyber security measures such as:

- Avoiding clicking on suspicious links and/or any attachments from websites, emails and text messages.
- Ensuring that your passwords to your personal accounts are long, random and complex. Do not use the same password over multiple accounts as once one account is breached, all other accounts that use the same password will likely be breached as well.
- By enabling two-step authentication with a one-time password may also help with preventing your password information from being stolen as one-time passwords are temporary and can only be used once.

Bibliography

Youtube.com. 2018. *Youtube*. [online] Available at: <https://www.youtube.com/watch?v=52WufHfjGP4> [Accessed 27 February 2020].

Keelog.com. n.d. *Hardware Keylogger - Keygrabber USB*. [online] Available at: <http://www.keelog.com/usb-keylogger/> [Accessed 27 February 2020].

Tsai, P., 2017. *What Is Keylogging? Definition, History, And How To Detect: Word Of The Week*. [online] The Spiceworks Community. Available at: <https://community.spiceworks.com/topic/2003395-what-is-keylogging-definition-history-and-how-to-detect-word-of-the-week> [Accessed 27 March 2020].

En.wikipedia.org. n.d. *Keystroke Logging*. [online] Available at: <https://en.wikipedia.org/wiki/Keystroke_logging#Use_by_police> [Accessed 27 March 2020].

Binance Academy. n.d. *What Is A Keylogger?* | *Binance Academy*. [online] Available at: <https://www.binance.vision/security/what-is-a-keylogger> [Accessed 27 March 2020].

Malwarebytes. n.d. *Keyloggers - What Is A Keystroke Logger?*. [online] Available at: <https://www.malwarebytes.com/keylogger/> [Accessed 27 March 2020].

Wu, T., Chung, J., Yamat, J. and Richman, J., 2020. *Keystroke Logging*. [online] The ethics (or not) of massive government surveillance. Available at: <https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/tech_keystrokelogging.html> [Accessed 27 March 2020].

DuPaul, N., n.d. *Keylogger*. [online] Veracode. Available at: <https://www.veracode.com/security/keylogger> [Accessed 8 April 2020].