KEYLOGGING

BE AWARE OF

WHAT IS A KEYLOGGER?

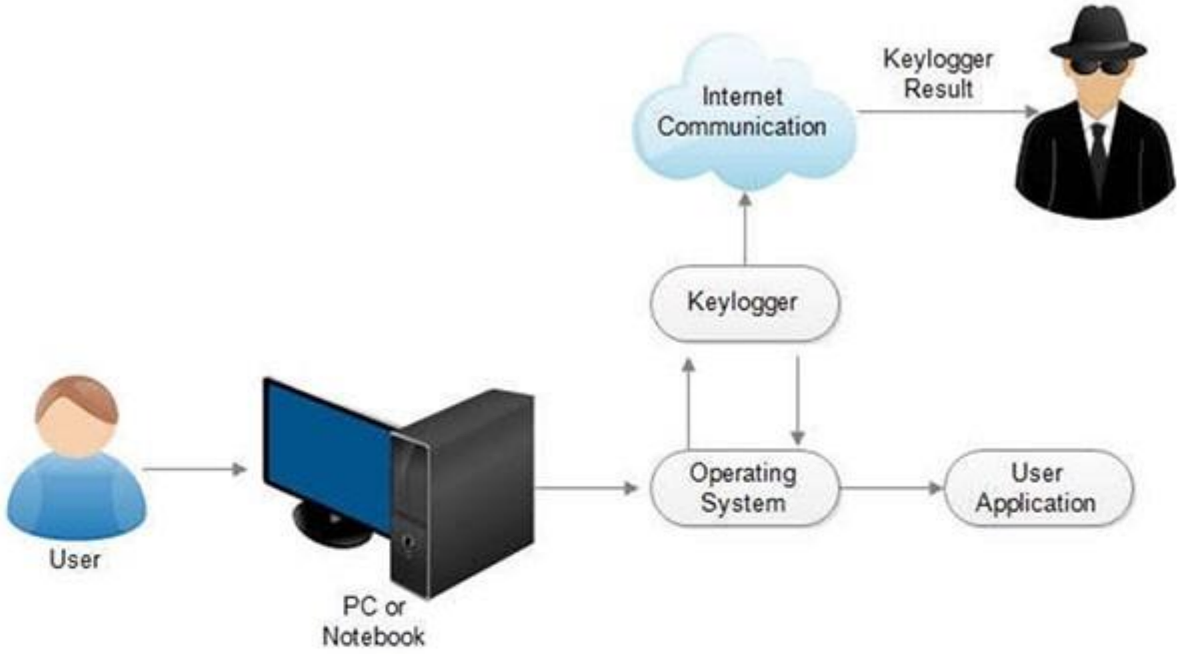
Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

HOW DO KEYLOGGERS WORK?

Keyloggers collect information and send it back to a third party – whether that is a criminal, law enforcement or IT department. “Keyloggers are software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques,” explains Tom Bain, vice president security strategy at Morphisec.

HOW KEYLOGGERS STORE DATA?

The amount of information collected by keylogger software can vary. The most basic forms may only collect the information typed into a single website or application. More sophisticated ones may record everything you type no matter the application, including information you copy and paste. Some variants of keyloggers – especially those targeting mobile devices – go further and record information such as calls (both call history and the audio), information from messaging applications, GPS location, screen grabs, and even microphone and camera capture.



TYPES OF KEYLOGGERS:

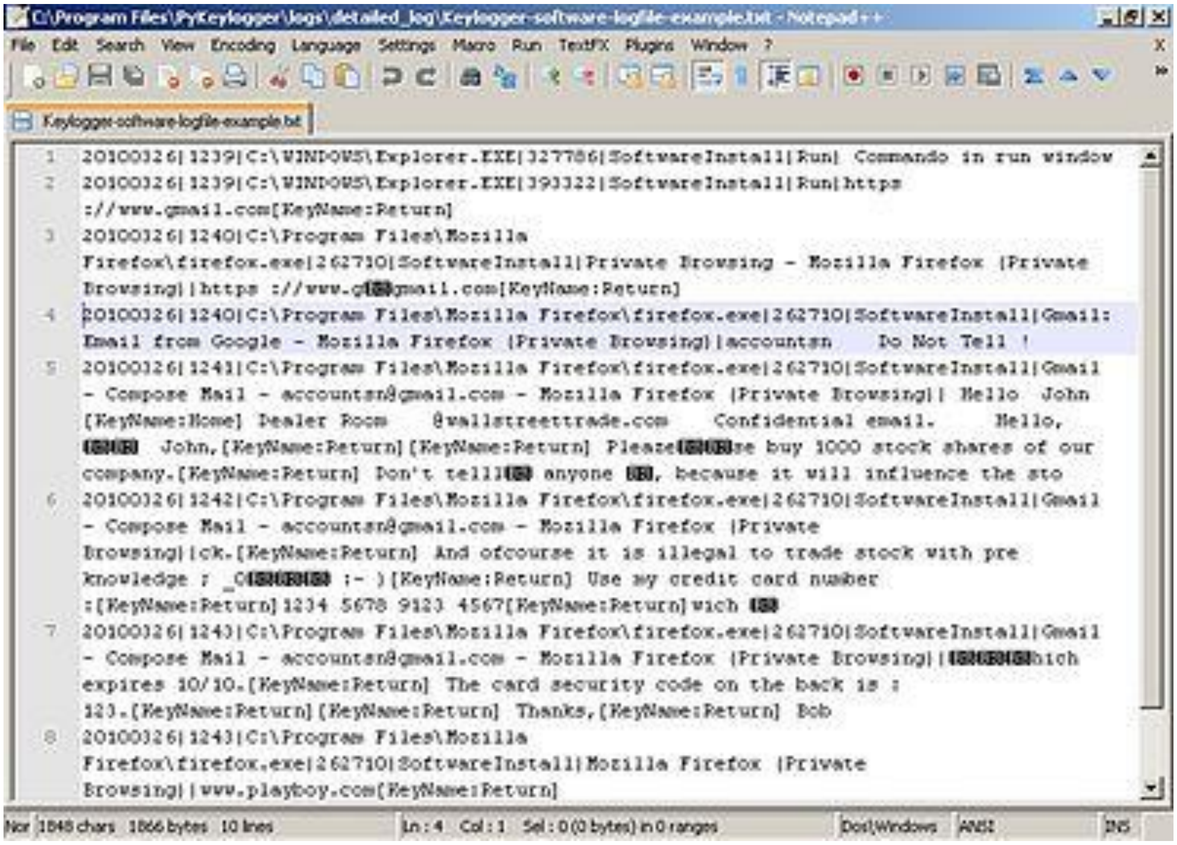
Keyloggers can hardware- or software-based. Hardware-based ones can simply nestle between the keyboard connector and the computer's port. Software-based ones can be whole applications or tools knowingly used or downloaded, or malware unknowingly infecting a device.

HOW KEYLOGGERS SEND DATA TO HACKERS?

Data captured by keyloggers can be sent back to attackers via email or uploading log data to predefined websites, databases, or FTP servers. If the keylogger comes bundled within a large attack, actors might simply remotely log into a machine to download keystroke data.

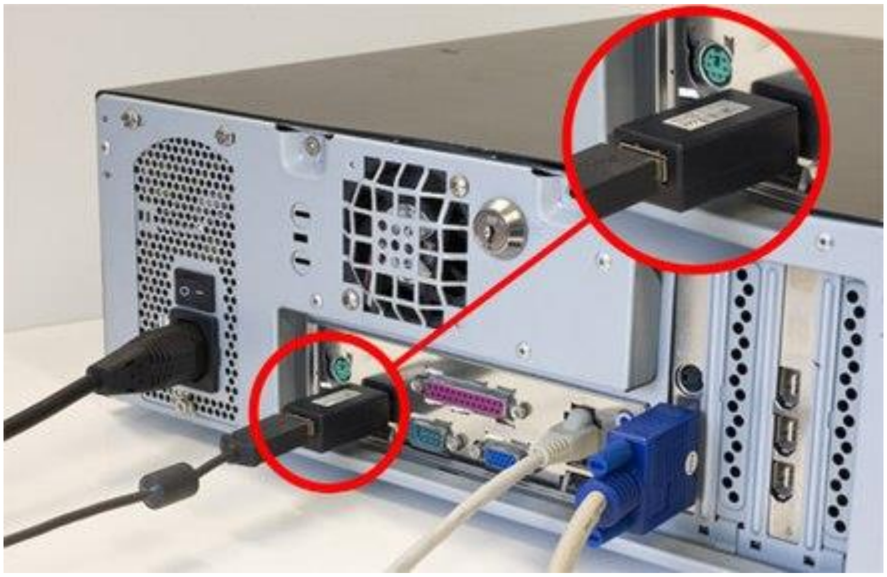
TYPES OF KEYLOGGERS (DETAILED):

1. **SOFTWARE BASED:**
   Software-based keyloggers are basically programs that plan to monitor your PC's working framework. The Keylogger shift in sorts and levels of framework infiltration. One case of which is memory infusion programming.


C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt
Nor 1848 chars 1866 bytes 10 lines
Ln : 4 Col : 1 Sel : 0 (0 bytes) in 0 ranges
Dos\Windows
ANSI
INS

```
20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https
://www.gmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private
Browsing)|https ://www.gBSgmail.com[KeyName:Return]
20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail:
Email from Google - Mozilla Firefox (Private Browsing)|accountsn    Do Not Tell !
20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello  John
[KeyName:Home] Dealer Room    @wallstreettrade.com    Confidential email.     Hello,
BSBS  John,[KeyName:Return][KeyName:Return] PleazeBSBSse buy 1000 stock shares of our
company.[KeyName:Return] Don't telllBS anyone BS, because it will influence the sto
20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private
Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre
knowledge ; _OBSBSBS :- )[KeyName:Return] Use my credit card number
:[KeyName:Return]1234 5678 9123 4567[KeyName:Return]wich BS
20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail
- Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|BSBSBShich
expires 10/10.[KeyName:Return] The card security code on the back is :
123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
20100326|1243|C:\Program Files\Mozilla
Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private
Browsing)|www.playboy.com[KeyName:Return]
```

2. **HARDWARE BASED:**
   Compared to a software-based Keylogger, hardware Keylogger doesn’t need any installing since they are as of now inside the physical system of the PC. Keyboard keyloggers are amongst the most widely recognized cases of hardware-based ones.



4 BEST PRACTICES FOR DETECTING AND REMOVING KEYLOGGERS:

1. Monitor resource allocation, processes and data

Observing resource allocation and background process on machines, as well as data being transmitted from the device outside the organization can help identify if a keylogger is present. Keyloggers usually need root access to the machine, which can also be a telltale sign of a keylogger infection.

2. Keep antivirus and anti-rootkit protection up to date

As keyloggers often come bundled with other forms of malware, discovering keylogger malware might be an indicator of a wider attack or infection. Up-to-date antivirus protection and anti- rootkit protectors will remove known keylogger malware, according to Jeff Wichman, practice director for Optiv Security, but may warrant further investigation to determine whether the keylogger was just one component of a larger attack.

3. Use anti-keylogger software

Dedicated anti-logger software is designed to encrypt keystrokes as well as scan for and remove known loggers and flag unusual keylogging-like behavior on the machine. Blocking root access for unauthorized applications and blacklisting known spyware apps will also help.

4. Consider virtual onscreen keyboards

Virtual onscreen keyboards reduce the chance of being keylogged as they input information in a different way to physical keyboards. This might impact user productivity, isn’t foolproof against all kinds of keystroke monitoring software, and doesn’t eliminate the cause of the problem.

thank you