Hardware Keyloggers

GIAC (GSLC) Gold Certification

Author: Glen Roberts, glen@glenroberts.com
Advisor: Chris Walker

Accepted: June 3, 2016

Abstract

Most information security professionals are familiar with keyloggers. However, while the security industry has produced plenty of defenses for software-based keyloggers, hardware keyloggers continue to pose a daunting problem for the typical enterprise. A deeper understanding of these insidious devices can lead to viable techniques for both protection and detection.

1. Introduction

The keyboard is one of the most commonly used and trusted devices on the planet for connecting humans to computers. So, why can't we keep them safe from attack?

hp KEYBOARD K1500
No distractions here. Quiet keys maintain peaceful work & play environments.
3 indicator lights glow green & illuminate your path to productivity.
Designed for comfort. Adjustable legs provide flexible wrist positions.
Full-size keyboard allows maximum productivity and precise accuracy.

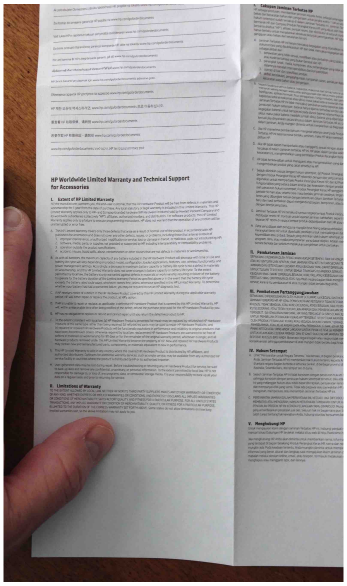
Keyboards have become a common focal point for attack by criminals wanting to copy sensitive information including authentication credentials. Most information security professionals are familiar with keyloggers, tools that attackers use to capture keystrokes for future playback. However, while the security industry has produced plenty of defenses for software-based keyloggers, hardware keyloggers continue to pose a daunting problem for the typical enterprise. A deeper understanding of these insidious devices can lead to viable techniques for both protection and detection.

2. The Problem with Keyboards

Along with the ubiquitous nature of keyboards comes their commoditization by manufacturers and consumers. Most consumers are unwilling to pay extra for commodity hardware, regardless of whether it includes security enhancements. Manufacturers, therefore, are not incented to improve the keyboard as needed to make it more secure.

In fact, most keyboard manufacturers (Microsoft, Apple, HP), while knowing about the vulnerabilities of their keyboards, refuse to assume liability for keyboard logging attacks and explicitly state they are not liable in their warranties. Unfortunately, most consumers and information technology professionals do not read these warranties.

The warranties are primarily provided to minimize risk to manufacturers. The small print provides a good indication of how much manufactures care about informing users of potential harm. For example, consider the size of the text in the picture below.



HP Worldwide Limited Warranty and Technical Support for Accessories

I. Extent of HP Limited Warranty

II. Limitations of Warranty

I. Cakupan Jaminan Terbatas HP

II. Pembatasan Jaminan

III. Pembatasan Pertanggungjawaban

IV. Hukum Setempat

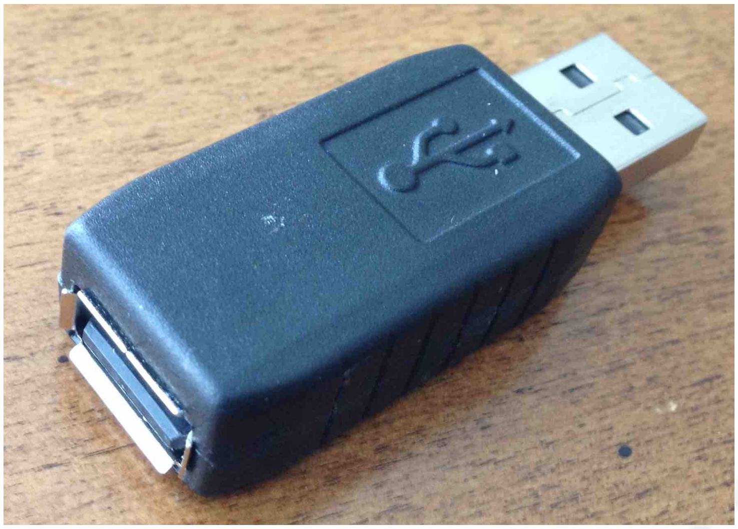
V. Menghubungi HP

The keyboard warranty pamphlet above (Hewlett Packard, 2012) states, “HP does not warrant that the operation of any product will be uninterrupted or error free.” It also states that it does not cover “unauthorized modification” or “malicious code not introduced by HP.” It even goes on to say that “in no event will HP or its third-party suppliers be liable” for any damages, “including any lost profits or savings.”

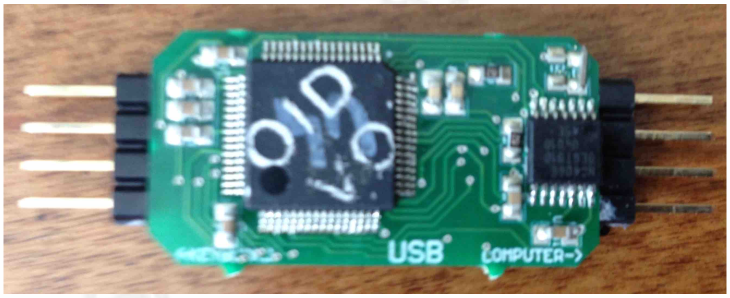
That is a fairly bold transfer of risk from the keyboard manufacturer to the average consumer. Most people, including IT employees, do not understand how insidious hardware keylogging truly is, much less how to protect their systems from such an attack. Due to a lack of security companies selling products to thwart these attacks, and the marketing efforts that usually accompany the sales process, hardware keyloggers receive far less attention than they deserve.

3. Types of Hardware Keyloggers

There are two predominant types of hardware keyloggers. The first is a keyboard adapter type that is installed inline by plugging the adapter into the keyboard and then plugging the keyboard into the adapter. Installed in this manner, it can easily intercept the traffic between the keyboard and the workstation. Note that this variety of keylogger comes in both PS/2 and USB flavors.



The other type of hardware keylogger is the module type that is actually a very small PCB. This device is installed inside the keyboard where it can evade detection. Installation takes more time and effort, but it is stealthy and provides the same functionality as the external adapter type. With this keylogger, security awareness training is less helpful than with the visible adapter type.



4. Hardware Keylogger Attacks

A hardware keylogger attack is so simple and can be carried out by individuals with virtually no knowledge of information technology much less security or penetration testing. There are so many ways to carry out these attacks. There are multiple attack possibilities with both external keyboard adapters and internally installed modules.

4.1. Keyboard Adapter Method

Imagine someone reaching over the retail counter when no one is looking and installing an external logger between the keyboard and the workstation or just casually setting one up at an isolated store kiosk. Keyloggers can be installed without detection by putting one on someone's computer while they retrieve a printout at the office printer. An attacker could even do the deed before or after work when no one is there to question it. It would be even easier to install them on new keyboards that are sold to the target company at a bargain.

4.1.1. Step 1: Unplug the Keyboard

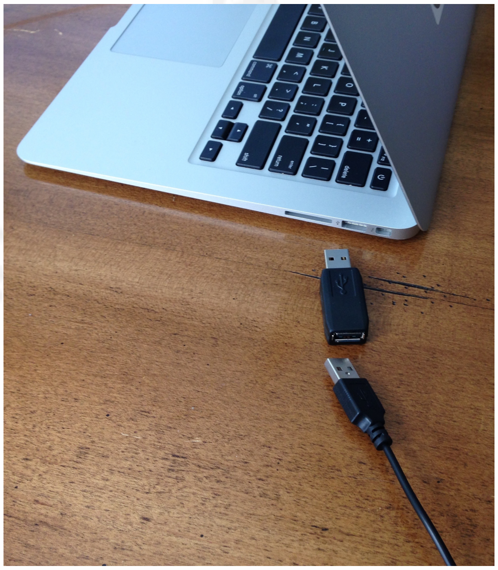
Trace the keyboard to the back of the computer and unplug the keyboard from the system.

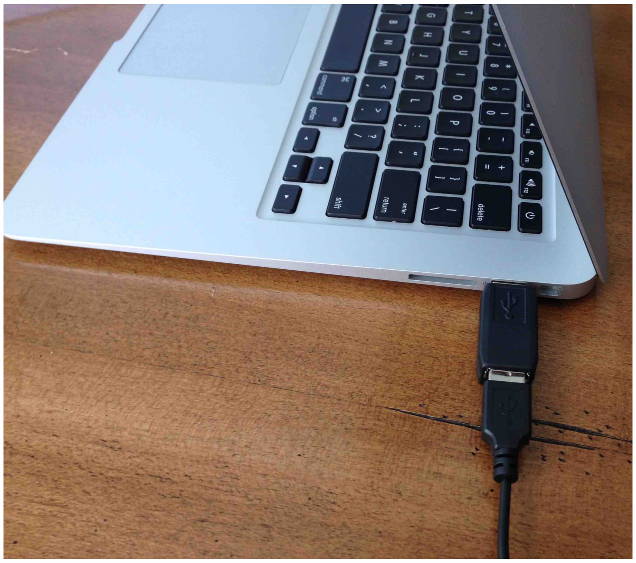
4.1.2. Step 2: Install the Keylogger

No tools are needed to install the keyboard adapter type of keylogger. Plug the keyboard is into the keylogger.

4.1.3. Step 3: Plug the Keylogger into the Computer

Lastly, plug the keylogger into the computer. This is the easiest type of keylogger to install, but it is also the easiest attack to spot sticking out of the computer. Although, some users think the keylogger is just a legitimate adapter of some sort.



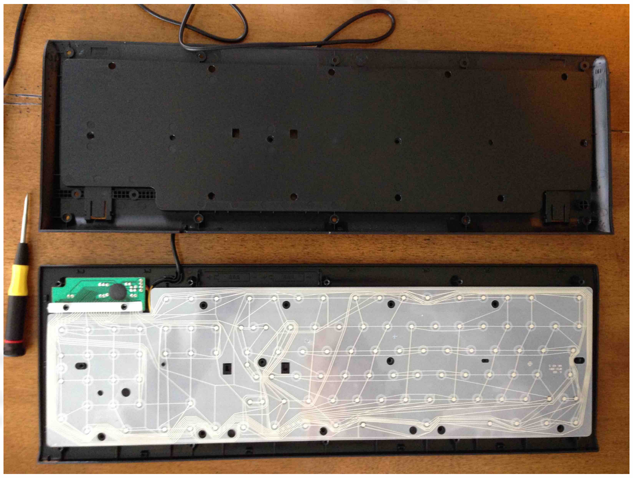


4.2. How Keyloggers are Installed Inside Keyboards

Performing a hardware keylogger attack with an internal module can take between five to ten minutes. You will need a few tools for the installation such as a small Phillips screwdriver, crimpers, pliers, wire cutters and DuPont connectors.

4.2.1. Step 1: Remove The Keyboard Cover

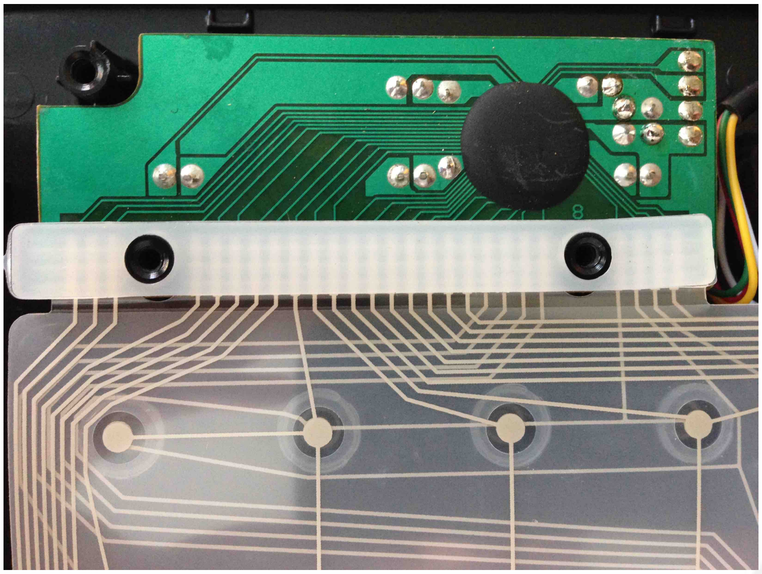
First, take off the keyboard cover by removing the Phillips screws on the back of the keyboard.

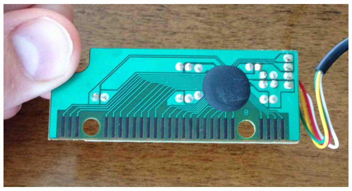


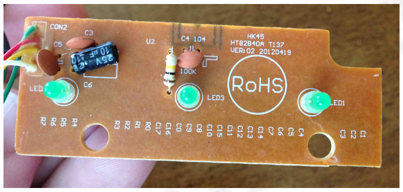
4.2.2. Step 2: Locate and Remove the Circuit Board

Next, locate the circuit board inside the keyboard. Trace the keyboard cable to quickly find it. Notice the circuit board is connected to a soft membrane, which interfaces with the keys. The circuit board is usually not screwed in. Pop it out and examine it.

Glen Roberts, glen@glenroberts.com

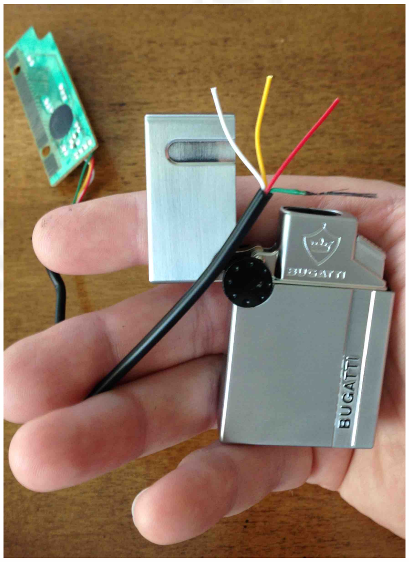






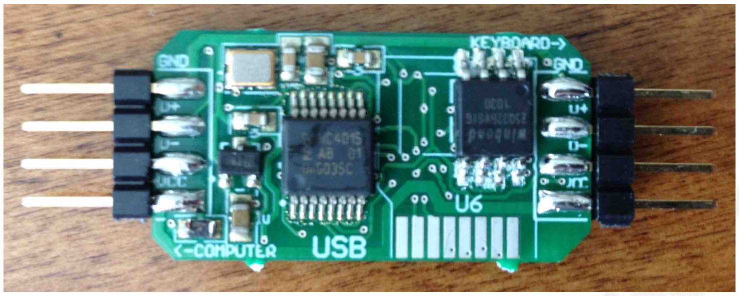
4.2.3. Step 3: Cut and Strip The Keyboard Cable

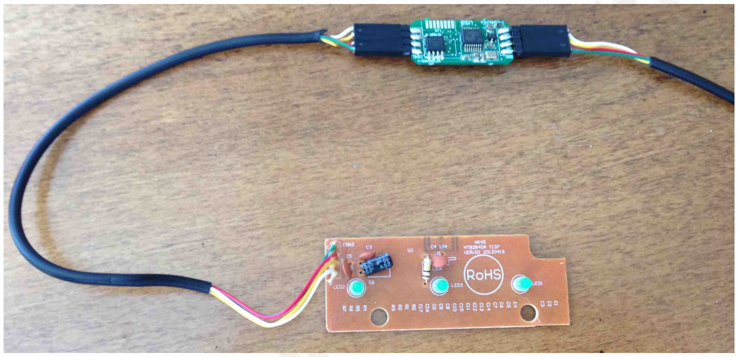
After removing the circuit board, cut the keyboard cable, leaving enough slack to play with later. Strip or burn off the insulation from the individual wires on both sides of the keyboard cable. This process includes the side connected to the circuit board and the side connected to the keyboard connector.



4.2.4. Step 4: Install the Keylogger Inline

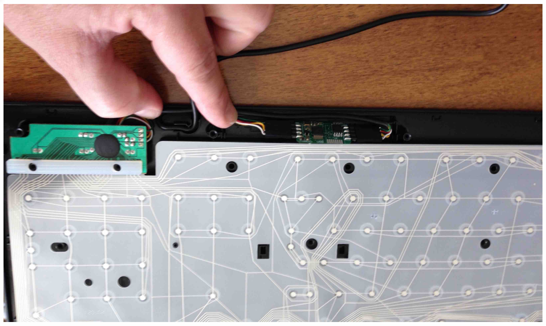
Finally, the keylogger is installed inline, thus reconnecting the keyboard cable. Connect each of the keyboard cable wires to the corresponding pin on the keylogger module such as GND, D+, D-, and VCC (KeyDemon, 2010). These pins are well labeled on the keylogger module and the keyboard's internal circuit board. In this example, I used DuPont connectors to connect the wires for ease of use, but the wires could just as easily have been connected using a soldering iron or superglue.





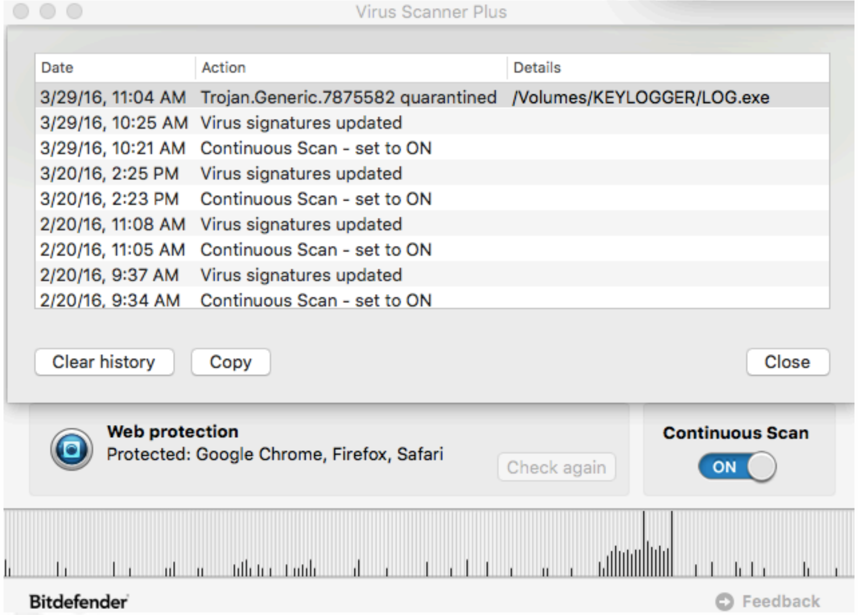
4.2.5. Step 5: Reassemble the Keyboard

For the final step, reassemble the circuit board inside the keyboard and wedge the keylogger in an empty compartment, towards the top of the keyboard. After everything is back in place, screw the keyboard cover back on. There is virtually no difference between the original keyboard and the modified keyboard, judging from outside appearances.



5. Hardware Keylogger Defense

For software keyloggers there are many layered defenses that include routine malware detection, web filtering, process whitelisting and port blocking (Tipton, 2010). Many of the general information security and software keylogger defenses also provide protection against hardware keyloggers. Examples include using dynamic passwords and safeguarding the physical environment by creating restricted areas. The supply chain should be controlled with reliable, well-vetted manufacturers and distributors of keyboards. Tamper protection can come in the form of system cages that prevent access to USB and PS/2 ports or Loctite, which can secure screws into keyboard covers. Lastly, malware protection may be able to stop software from being implemented from keyloggers. For example, Virus Scanner Plus blocked software run from a keylogger as shown below.



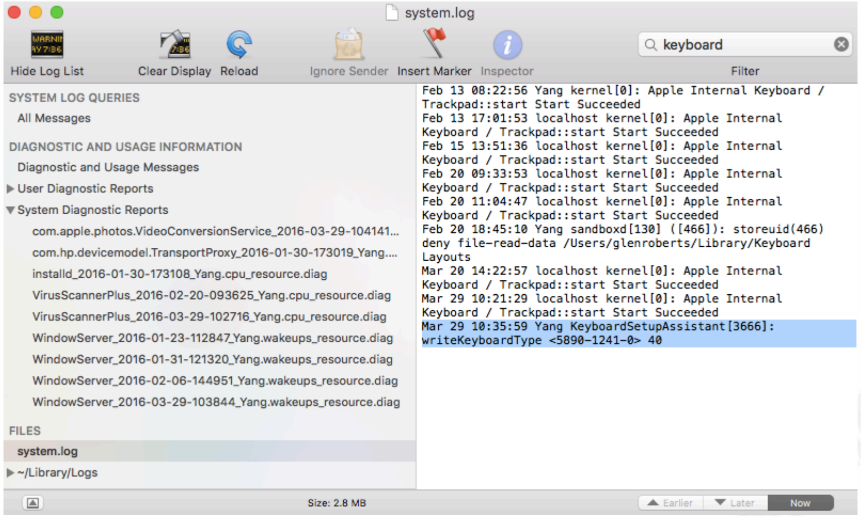
Virus Scanner Plus

Date	Action	Details
3/29/16, 11:04 AM	Trojan.Generic.7875582 quarantined	/Volumes/KEYLOGGER/LOG.exe
3/29/16, 10:25 AM	Virus signatures updated	
3/29/16, 10:21 AM	Continuous Scan - set to ON	
3/20/16, 2:25 PM	Virus signatures updated	
3/20/16, 2:23 PM	Continuous Scan - set to ON	
2/20/16, 11:08 AM	Virus signatures updated	
2/20/16, 11:05 AM	Continuous Scan - set to ON	
2/20/16, 9:37 AM	Virus signatures updated	
2/20/16, 9:34 AM	Continuous Scan - set to ON	

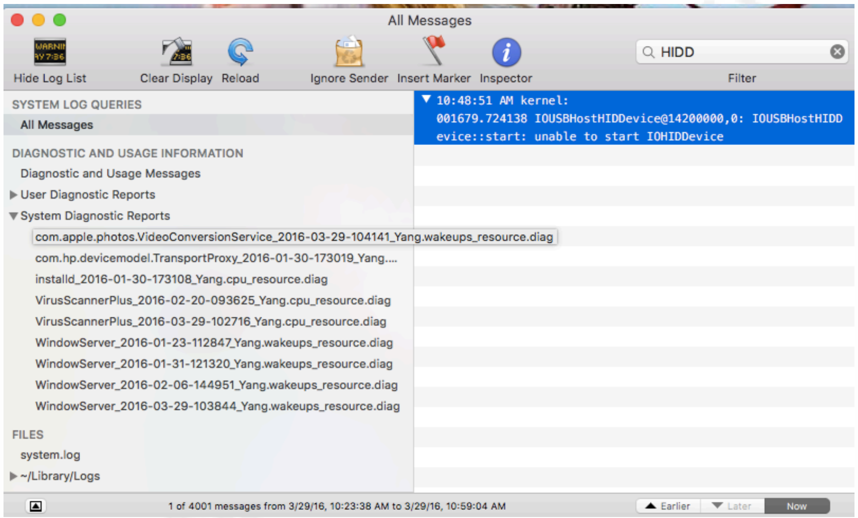
Web protection
Protected: Google Chrome, Firefox, Safari

Continuous Scan: ON

For detective measures, security awareness training is always helpful. Also, defensive-sweeps can be conducted periodically to look for keyloggers between keyboards and computers. Logs can be reviewed for entries indicating a keyboard was disconnected, connected or whether a system has been shutdown and restarted. For example, logs can be used to detect keyboards that are plugged in and software that is executed.


system.log
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
keyboard
Filter
SYSTEM LOG QUERIES
All Messages
DIAGNOSTIC AND USAGE INFORMATION
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
com.apple.photos.VideoConversionService_2016-03-29-104141...
com.hp.devicemodel.TransportProxy_2016-01-30-173019_Yang....
installd_2016-01-30-173108_Yang.cpu_resource.diag
VirusScannerPlus_2016-02-20-093625_Yang.cpu_resource.diag
VirusScannerPlus_2016-03-29-102716_Yang.cpu_resource.diag
WindowServer_2016-01-23-112847_Yang.wakeups_resource.diag
WindowServer_2016-01-31-121320_Yang.wakeups_resource.diag
WindowServer_2016-02-06-144951_Yang.wakeups_resource.diag
WindowServer_2016-03-29-103844_Yang.wakeups_resource.diag
FILES
system.log
~/Library/Logs
Size: 2.8 MB
Earlier
Later
Now

```
Feb 13 08:22:56 Yang kernel[0]: Apple Internal Keyboard /
Trackpad::start Start Succeeded
Feb 13 17:01:53 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Feb 15 13:51:36 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Feb 20 09:33:53 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Feb 20 11:04:47 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Feb 20 18:45:10 Yang sandboxd[130] ([466]): storeuid(466)
deny file-read-data /Users/glenroberts/Library/Keyboard
Layouts
Mar 20 14:22:57 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Mar 29 10:21:29 localhost kernel[0]: Apple Internal
Keyboard / Trackpad::start Start Succeeded
Mar 29 10:35:59 Yang KeyboardSetupAssistant[3666]:
writeKeyboardType <5890-1241-0> 40
```


All Messages
Hide Log List
Clear Display
Reload
Ignore Sender
Insert Marker
Inspector
HIDD
Filter
SYSTEM LOG QUERIES
All Messages
DIAGNOSTIC AND USAGE INFORMATION
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
com.apple.photos.VideoConversionService_2016-03-29-104141_Yang.wakeups_resource.diag
com.hp.devicemodel.TransportProxy_2016-01-30-173019_Yang....
installd_2016-01-30-173108_Yang.cpu_resource.diag
VirusScannerPlus_2016-02-20-093625_Yang.cpu_resource.diag
VirusScannerPlus_2016-03-29-102716_Yang.cpu_resource.diag
WindowServer_2016-01-23-112847_Yang.wakeups_resource.diag
WindowServer_2016-01-31-121320_Yang.wakeups_resource.diag
WindowServer_2016-02-06-144951_Yang.wakeups_resource.diag
WindowServer_2016-03-29-103844_Yang.wakeups_resource.diag
FILES
system.log
~/Library/Logs
Earlier
Later
Now

```
▼ 10:48:51 AM kernel:
  001679.724138 IOUSBHostHIDDevice@14200000,0: IOUSBHostHIDD
  evice::start: unable to start IOHIDDevice
```

1 of 4001 messages from 3/29/16, 10:23:38 AM to 3/29/16, 10:59:04 AM

6. Conclusion

Understanding how hardware-based keyloggers are implemented is invaluable to information security professionals. It is important for security professionals to remember that, just like software-based keyloggers, hardware keyloggers are also defendable. Building these defenses into a security program can help prevent and detect these keylogger exploits.

References

KeyDemon. (2010). *KeyDemon Module User's Guide*. Wroclaw: KeyDemon.

Hewlett-Packard. (2012). *HP Worldwide Limited Warranty and Technical Support for Accessories.* China. Hewlett-Packard Development Company, L.P.

Tipton, H. (2010). *Official (ISC)^2 Guide to the CISSP CBK, Second Edition*. Boca Raton: Auerbach Publications.