KEY LOGGER: A MALICIOUS ATTACK

Mr. Shubham Tiwai
MCA 6thSem
Deptt: Computer Application
UIM, Uttaranchal University
Dehradun, Uttarakhand

Mr. Shubham Bhat
MCA 6thSem
Deptt: Computer Application
UIM, Uttaranchal University
Dehradun, Uttarakhand

Mr. Ravi Kumar Singh
MCA 6thSem
Deptt: Computer Application
UIM, Uttaranchal University
Dehradun, Uttarakhand

Abstracts: Key logger is type of a rootkit Malware that capture typed Keystroke event of the keyboard and save into logfile. Therefore, it is able to intercept sensitive information such as usernames, pins and password. Thus transmits into malicious attacker without attracting the attention of users. Key loggers presents a major threat to business transactions and personal activities such as E-Commerce, online Banking, Email and Database. Antivirus Software I commonly used to detect and remove known Key loggers. This Paper Presents an introduction of Key logger, types and characteristics of key loggers and methodology they use.

Keywords:
Hooking, Signature-Based, Malware Rootkits, Anomaly Based, Detection of Keylogger, Security, Works of key logger.

I. INTRODUCTION

Malware is termed by numerous Names, Such as Malicious code (MC), Malicious Software and Miscode. Malicious code as any code added, changed, or removed from a software system. Key logger is one of malware Rootkits that intercepts the user's typed Keystroke on the keyboard. The first primary target of the Key logger is to secretly record confidential information of user's input through Keystroke monitoring and them relaying this valuable information to others the keyboard is the focal method of inputting textual and numerical information on the computer through typing. Therefore an attacker can simply retrieve and access important information with the help of logging keystrokes.
Nowadays, Key logging acts a critical threat to the security and privacy of our system. These causes of the Key logger Program can retrieve and collect the user's personal information, credits card, password performed by Hacker. The stealthy key logger cannot be detected by any Antivirus Software as running on the victim's machine. The user has no way to determine the presence of key logger on his machine. Therefore he turns into a victim of the identity theft. Access important information with the help of logging Keystrokes.
Therefore different type of key loggers divided into two main groups Hardware Key loggers and Software Keyloggers.

II. TYPES OF KEY LOGGER

1. Hardware Key logger: - Hardware Key loggers are used small electronics device used for capturing the data in between a keyboard device and I/O Port.

Usually these devices have built in memory where they store the key stroke so this means that must be retrieved by the person who installed it in order to obtain the information. An advantage of these key loggers is that they are undetectable by anti-viral software or scanners since it works on the Hardware platform.
Software key logger tracks the system, collect keystroke data within the targeted operating system. It store that on the disk or in remote locations and send that data to the attacker who installed the key logger .A key logger Spyware is a different kind of malware attack which uses two malwares program in a combined script. There are multiple way to stole or hack user's confidential credentials and sensitive data. Key logger is one of the most frequently used methods to obtain user's information.

Hardware key logger is physical device located between the keyboard and the computer. There are two connection methods. Key loggers can be connected between the keyboard and computer or computer directly.

key logger of ps\2

The second method does not require physical connection to the PC. But Installation of key logger circuit into the keyboard standard. This method has advantage that users cannot maintain key logger physically.

1.1 Wireless Keyboard:

Wireless keyboard exploits Bluetooth interfaces to transfer captured data to a log file up to the distance of 100m [4]. The primary target of this wireless key logger is to intercept transmitted packet from wireless key logger keyboard that uses 27 MHz connect to the keystroke.

Bluetooth-accessible key logger

1.2 Acoustic Key logger:

Unlike usual Key logger, acoustic key logger works on analysis and captures the sound of indivisual keystrokes. Special equipment is required to the sound of the user's typing. Like microphone is used to pick up the keyboard sound from hundred feet away of target area or work [5].

2. Software Key logger:

Parasite reported a total of 540 key loggers and they were mostly software based. Window operating system has many event mechanisms. For example when a character is pressed on the keyboard or mouse clicked, the keyboard driver on the operating system translates this event into window message called WM-KEYDOAWN. This message is pushed into system message queue for the transmission of message.

Software key logger can be categorized as follows:

2.1 Interrogation cycle software key logger:

This type of key logger is simplest and can easily been detected. It uses a number of API functions to return information into variables and custom function to return character during function call processing [6]. These functions interrogate keys on the keyboard. For instances if a key is pressed or released, the Getkey function is then called from the Getkey board state and determine information. Get keyboard Statecopies the status of the 256 virtual keys to the specified buffer storage.

2.2 Traps Software Key logger:

This mechanism works only for GUI application to trap not only the keystroke themselves but messages that are processed in window of other GUI application as well.

2.3 Rootskits Software Key logger:

The rootkit software key loggers are the most dangerous type of key logger. But it is a relatively rare. It captures set of functions responsible for information. There are two distinct types of hooks related to windows message. Keyboard hook are-

- Reading all keyboard message and transfer them to the next hook procedure in a chain. Modify the original message and pass it to the next hook procedure.
- Responsible for interrupt to the flow of the message by not passing it to the next hook procedure.

2.4 Kernel-Mode software key loggers:

Generally, most of the key logger use kernel mode technique that based on standard principles, installing a driver filter for the keyboard driver. This provides spyware to connect keyboard drive stack with the help IO attach device and IO create device that starts functioning automatically after loading the operating system.

III HOW KEY LOGGER WORKS

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

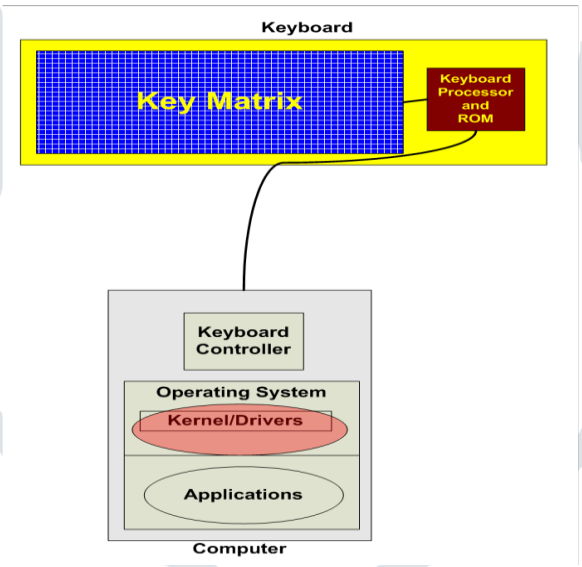
- Quality assurance testers analysing source of system errors.
- Developers and analysts studying user interaction with system.
- Employee monitoring and
- Law enforcement or private investigators looking for evidence of an ongoing crime or inappropriate behaviour.

On the other side of the line between lawful and unlawful use, cybercriminals use key logging technology to capture identities, confidential, password and any other marketable information.

➢ Software Key logger:

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.

A portion of the logger resides in the OS kernel and receives data directly from the keyboard interface. It replaces the kernel component that interrupts key strokes. The read area shows the location of a kernel-based key logger in the keystroke-to-operating system path.



Both types of software key loggers intercept keyboard data, write a copy to a local file with encrypted data, and then forward information to the operating system. Anti-malware or personal firewall host-based intrusion prevention (HIPS) solutions detect and remove applications of key loggers. Kernel-based solutions are not so easy to find, although prevention controls like HIPS can prevent their implementation.

➢ Hardware Key loggers

A hardware key logger is essentially a circuit based located in between the keyboard and the computer devices placed inline means of deployment.

PS2 key logger

USB key logger

One method is about Key logger that is connected directly to the PC and the Keyboard. Another method is to install a key logger circuit into a standard keyboard. This has the advantage of no physical evidence of user monitoring. Laptop presents a special challenge, external key logger is not an option unless the portable computer never leaves its docking station and an external keyboard is used. So devices must be installed in the laptop. Figure is an example of a mini-PCI hardware key logger.

laptop key logger

Physical access or proximity is required when using a hardware key logger, for installation and to external captured data. Let's step through the process. Once the key logger is connected, it immediately begins keystroke collection, powered by the PC connector. A processor on the logger captures character and control code data and writes them to onboard memory. Memory capacity often exceeds 4 GB, enough to store up to two years of typing. This process is invisible to the user and impossible to detect. The key logger stores no files on the target system nor does it require tell-tale software. Data is extracted from key logger storage in one of two ways. In the first method, a keystroke combination on the target system's keyboard loads and executes a menu stored on the key logger.

KeyGhostpassword

[C] safe mode

.....

KeyGhost II Standard v6.3.8
www.keyghost.com

Menu >

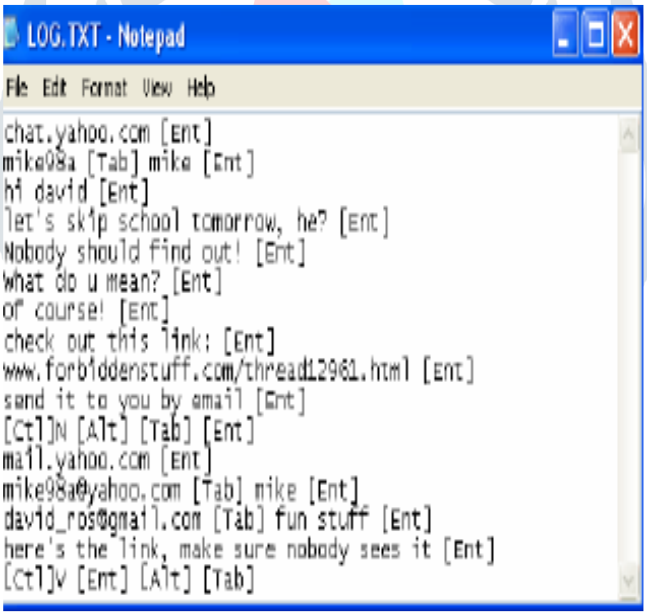
1) Entire log download
2) 2) Section log download
3) 3) Wipe log
4) 4) Format memory
5) 5) Options
6) 6) Optimize speed
7) 7) Password change
8) 8) Diagnostics
9) 9) eXit

Select > 1

- key to stop –

Fig- sample hardware key logger menu

As shown, the key logger password and log are managed from the machine to which it's attached either the target system or an offsite analysis device. The log can be downloaded to any attached storage device. In this Figure shows sample log content.



The log Stored in the key logger's memory is accessed via any of the following-

- All laptops and Desktops running windows 98, 2000, XP, Vista.
- Running MAC OS 8\9, OSX.
- All mobile phones running windows mobile and
- The iphone.

IV CONCLUSION:

Key loggers are powerful tools that cannot threat the system itself, but the user's confidential data such as user name, password, pin and card bank. In this paper we have shown different password attacks. as key logger is also one kind of password attack. Also we described what is key logger one can get access to our valuable. Information and to our personal system so, detection and prevention of key logger is highly desirable. In this paper we have enlist some of the prevention and detection method for key logger. In this paper we have understand how key logger works. Also we have described what is key logger and different types of key logger. The discussed attacking scenario is very threatening it is making a combination of two malware i.e. - key logger and spyware. It can steal the credentials or any confidential information typed can be leaked. In this system the detection is performed by the help of malware and keystroke agent. The prevention is performed by the help of encryption Algorithm.

V REFERENCES:

[**1**] http://securityresearch.in/index.php/projects/malware_lab/malware-keyloggers/

[2] http://www.ijcsmc.com/docs/papers/March2013/V2I3201322.pdf

[3] http://www.wellresearchedreviews.com/computer-monitoring-software-reviews.html

[4] http://blog.opensecurityresearch.com/2012/10/hacking-keyloggers.html

[5] http://www.keylogger.org/

[6] http://christopherwood.com/papers/KeyloggersInCybersecurityEducation.pdf

[7] http://securityresearch.in/index.php/projects/malware_lab/malware-keyloggers/

[8] http://www.ijcsmc.com/docs/papers/March2013/V2I3201322.pdf

[9] http://adventuresinsecurity.com/images/Keystroke_Logging.pdf

[10] http://en.wikipedia.org/wiki/Keystroke_logging Keylogging history.