Watchdroid

Submitted in partial fulfillment of the requirements

For the degree of

Bachelor of Engineering by

Pratima Gaikwad.

Roll No. 11

Aarti Gauda.

Roll No. 12

Mayur Zanzane.

Roll No. 64

Under the supervision of

Prof.Mahesh Zemse

DEPARTMENT OF INFORMATION TECHNOLOGY

KONKAN GYANPEETH COLLEGE OF ENGINEERING

Konkan Gyanpeeth Shaikshanik Sankul, Vengaon Road,

Dahivali, Karjat Dist. Raigad-410201

Academic Year- 2020-21

Certificate

This is to certify that the project entitled **Watchdroid** is a bonafide work of **Pratima Gaikwad(Roll No. 11), Aarti Gauda(Roll No. 12), Mayur Zanzane(Roll No. 64)** submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **Undergraduate** in **DEPARTMENT OF INFORMATION TECHNOLOGY.**

Supervisor/Guide

Prof. Mahesh Zemse

Department of Information Technology

Head of Department

Prof. A. S. Kunte

Department of Information Technology

Principal

Dr. M. J. Lengre

Konkan Gyanpeeth College of Engineering

Project Report Approval for B.E.

This thesis / dissertation/project report entitled **Watchdroid** by **Pratima Gaikwad(Roll No. 11), Aarti Gauda(Roll No. 12), Mayur Zanzane(Roll No. 64)** is approved for the degree of **DEPARTMENT OF INFORMATION TECHNOLOGY**.

Examiners

1._____

2._____

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original Sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in My submission. I understand that any violation of the above will be cause for disciplinary Action by the Institute and can also evoke penal action from the sources which have thus Not been properly cited or from whom proper permission has not been taken when needed.

Signature

Pratima Gaikwad (Roll No. 11)

Signature

Aarti Gauda (Roll No. 12)

Signature

Mayur Zanzane. (Roll No. 64)

Date:

INDEX

ABSTRACT

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 for 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 key logger 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.

INTRODUCTION

Keyloggers have somewhat of a bad reputation in the technology world because more often it's associated with illegal spying and theft of personal and monetary information. In reality even though that's one of the main uses, it can be used for other more appropriate and legal tasks. One clear example of this would be at a company's security policy which clearly states that the workers activities can be monitored with Keylogger and can be used to monitor an employee who is under suspicion of being a malicious insider.

Keystroke logging, often referred to as key logging or Keyboard Capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It also has very legitimate uses in studies of human-computer interaction. There are numerous key logging methods, ranging from hardware and software-based approaches to acoustic analysis. This project refers to a software based key logger.

There are two main goals of this project,

1. To develop the key logger.
2. To develop a new password protection system

Key Loggers are computer programs designed to work on the target computer's operating system as well as on android OS.

HISTORY OF KEYLOGGERS

Keylogging, often referred to as Keyboard Capturing or Keystroke logging, is the action of recording or monitoring every key pressed on a keyboard. Even though these devices are relatively new to us, Keyloggers have already been with us almost half of a century. Their exact history cannot be known perfectly, for it is believed that they first were used by the government and obviously they do not release any exact day.

In fact, it can be established that the first terrorists' cyber-attacks started with Keylogging activities. In Moscow and St. Petersburg spies started installing Keyloggers in the US Embassy and Consulate buildings in 1970, as a method of capturing information to be used in malicious manner. Another anecdote about Keylogging actions goes to November, 1983, when an early keystroke logger written by Perry Kivolowitz was posted to the Usenet news.

This posting appears to be a motivating factor in restricting access on UNIX systems. As it can be seen, Keylogging activities were directly related to governmental monitoring. However, since the beginning of the 21st century, Keyloggers have become one of the most technology devices used for surveillance, government wide and beyond.

SECURITY

Security using Keyloggers will monitor email, internet, chats or anything that requires a keystroke. This will help capture all information in text form. Keyloggers are a type of malicious malware that track the users' keystrokes and captures the characters that are pressed in and writes the information to a file. Even though that both hardware and software Keyloggers are known, software Keyloggers are the ones that are being widely used due to the inexpensive and easier to implement onto a computer. Each different operating system will have an adapted Keyloggers which suits the I/O.

Monitoring keystrokes will help with the work flow, investigation theft, review performance, prevent harassment, missing data and prevent personal use. Work flow will increase due to the fact that the employees will be motivated, this will weed out the employees that want to go on Facebook or check their personal emails which might cause a security leak. If there is some type of deleted file or missing information the security personnel can detect which computer that is missing such important information and figure out what went wrong. Employees knowing all this will show performance at their job from the amount of keystrokes they had to do. If someone is being harassed then this will increase the chances of finding out whom and when the incident occurred. In the end this will prevent personal use and increase safety and security with other benefits.

WatchDroid application has a in building protection mechanism which will help to keep all the recorded keystroke log save and secure from unauthorized access.

Locker has traditional pin method with a small change. The user has to set 2 positions and in that position he has to enter two numbers which will be set as password numbers for the application. When the user tries to open the app he will be asked to enter a password.

When the user enters the correct number in correct position then and then only app will be unlocked.

For Example - The user sets first position at 2 and at that position sets 4 as a password and second position as 3 and at that position sets number 6 as password, so while entering the password user has to enter 4 and 6 at correct positions. User can use many combinations to enter password which will confuse others who are trying to see users password.

IMPLEMENTATION

The implementation of Keylogger and design are based upon many factors: the type of operating system, the lifespan of a Keylogger.

In our case, whenever user clicks on an edittext a link between the log file and keyboard is created, and current time and date gets printed at start of line in log file. When the user clicks on a character or a number on the keyboard, the ASCII value of the pressed key is fetched and is written in the log file (real char is written in log not ASCII value).

CONCLUSION

x

This paper went over most issues regarding Keystroke logging. Although Keyloggers have a bad reputation in society, the research done to elaborate this paper shows how these devices can be used not always in a malicious way of action such as illegal spying and theft of personal information.

At a company level, Keyloggers can be used to monitor any suspicious activity that may cause a serious liability to the company's benefit. Workers who are under doubt can be explicitly be discover or clear their names. This helps the company ensure their interests before any bigger security issue happens, making them save larger quantities of money. Another legal way of using a Keylogger is in a closer and more personal level, home. Any head of household wants their children going on the internet without any consent of what they are watching, what websites are they surfing in, and most important who they are in contact with.

Nowadays, there are a lot of people looking for victims online. Child's predator, kidnappers, and so all are always seeking innocent children, and Keyloggers can be very helpful in order to minimize those kinds of attacks from occurring. In this paper it is also discussed the different kinds of Keyloggers and their advantages compared to one another. The Keystroke loggers can be divided into 2 main groups Hardware Keyloggers and Software Keyloggers. The main advantage of hardware Keyloggers is that they are invisible to any antiviral software or scanner.

How our Keylogger POC 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: ¾ Quality assurance testers analyzing sources of system errors; ¾ Developers and analysts studying user interaction with systems; ¾ Employee monitoring; and ¾ 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 keylogging technology to capture identities, confidential intellectual property, passwords, and any other marketable information. Keyloggers 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 keyloggers 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 Keyloggers Software keyloggers 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 keylogger, users participated in some way in the software's installation. Keylogging applications use a hooking mechanism (e.g., SetWindowsHookEx()) to capture keyboard data. Vendors often package solutions, like Perfect Keylogger, as an executable or a DLL (Shetty, 2005). Most kernel-based keyloggers 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 interprets keystrokes (Shetty, 2005). The red area in Figure 3 shows the location of a kernel-based keylogger in the keystroke-to-OS path. Figure 3: Kernel-based Keylogger Both types of software keyloggers 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. Anti-malware, personal firewall, and host-based intrusion prevention (HIPS) solutions detect and remove application keyloggers. Kernel-based solutions are not so easy to find, although prevention controls like HIPS can prevent their implementation. Installed as part of a rootkit package, kernel-level loggers elude anti-malware detection. Further, they don't show up in the list of running processes. Only rootkit detection software (e.g., RootkitRevealer) can detect, report, and help remove them. However, rootkits once installed are almost impossible to eradicate. If detected, remediate with a complete reinstall of the infected system. Other detection methods include: ¾ Scan local drives for log.txt or other log file names associated with known keyloggers; ¾ Implement solutions that detect unauthorized file transfers via FTP or other protocols; ¾ Scan content sent via email or other authorized means looking for sensitive information; ¾ Detect encrypted files transmitted to questionable destinations. Software keyloggers can be detected using software tools. For this reason, users of keyloggers often prefer hardware solutions. Hardware Keyloggers A hardware keylogger is essentially a circuit located somewhere between the keyboard and the computer (en.wikipedia.org/wiki/Hardware_keylogger). Devices placed inline with the keyboard cable are the most popular means of deployment. Figure 4 shows two variations of PS/2 keylogger and Figure 5 a USB type. Figure 4: PS2 Keyloggers (SpyCop) Figure 5: USB Keylogger (Keelogger) In both cases, the keylogger is connected directly to the PC and the keyboard to the keylogger. Another method is to install a

keylogger circuit into a standard keyboard. This has the advantage of no physical evidence of user monitoring. Laptops present a special challenge. External keyloggers are 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 6 is an example of a mini-PCI hardware keylogger. Figure 6: Laptop Keylogger (BitForensics) Physical access or proximity is required when using a hardware keylogger, for installation and to extract captured data. Let's step through the process. Once the keylogger 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 keylogger stores no files on the target system nor does it require tell-tale software. Data is extracted from keylogger memory 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 keylogger. See Figure 7. Figure 7: Sample Hardware Keylogger Menu (KeyGhost) As shown, the keylogger's password (key combination) 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. Figure 8 shows sample log content. Figure 8: Sample Log File Content (Keelogger) The previous retrieval method requires actual physical contact with the target system or the keylogger. However, there is another way. See Figure 9. Figure 9: Bluetooth-accessible Keylogger (Wirelesskeylogger.com) Wirelesskeylogger.com offers a Bluetooth-accessible keylogger, capable of transmitting up to 300 feet, through walls and other physical structures (wirelesskeylogger.com). Although only available for PS/2 connections, the site states that USB support is in the works. It also comes in a wireless keylogger keyboard. The log stored in the keylogger's memory is accessed via any of the following: ¾ All laptops and desktops running Windows 98, 2000, XP, Vista; ¾ All laptops and desktops running MAC OS 8/9, OSX; ¾ All mobile phones/PDA's running Windows Mobile; and ¾ The iPhone. The advantage of using a hardware keylogger is its invisibility to anti-malware software; although security aware users can easily see them. A disadvantage, at least for nonBluetooth-accessible devices, is the need for physical access to retrieve information. Bluetooth keyloggers are visible to Bluetooth detection solutions. However, wirelesskeylogger.com claims it can help. Physical access and AV software detection challenges are also addressed by the last two keylogger types. The first is wireless keyboard intercept. Wireless Keyboard Intercept For the purpose of this paper, wireless keyboards are devices that use a 27 MHz RF connection. The good news is that transmission range is limited to six feet. The bad news is that there is an RF transmission radius of six feet. And although wireless keyboard manufacturers encrypt RF transported keystroke characters, the encryption, at least on Microsoft keyboards, is very weak (Moser and Schrodel, 2008). Do not rely on it to protect sensitive data. What makes this a serious problem, even with a six foot limitation, is an attacker's capability to capture packets from all wireless keyboards within range, at the same time. Each packet is flagged so the keyboard's receiver knows to process it. This also allows an RF device to sort captured wireless keyboard packets into appropriate character streams. The one big disadvantage of using wireless intercept keyloggers is the need for a receiver/antenna relatively close to the target system. However, it's easy to hide small antennas in most office environments. The point to take away? If a workstation is processing highly sensitive information, don't use 27 MHz wireless keyboards. And physical security is always a good control. Acoustic Keyloggers The final keylogger type is like something out of a James Bond movie. It requires special equipment that "listens" to a user typing and special

software that performs statistical analysis on captured data. Acoustic logging technology is more experimental than practical, based on work done at the University of California, Berkeley (Zhuang, Zhou and Tygar, 2005). Let's see how it works. The same devices used to remotely listen to conversations are used to record typing sounds. Such microphones can be placed in the target work area or long distance solutions can be used. Parabolic microphones are an example of a long distance device. See Figure 10. Figure 10: Parabolic Microphone These microphones can pick up keyboard sounds from hundreds of feet away. Attached equipment records the sounds, which are then passed to audio-to-character translation software. The software uses the statistical constraints of English, i.e. "the limited number of English words limiting the possible temporal combinations of keys and English Grammar limiting the word combinations" (Zhuang, Zhou and Tygar, 2005). Using a 10 minute sound recording of a user typing English text, it takes about 30 minutes to derive character results. The process correctly translates 75 to 90 percent of words typed and 90 to 96 percent of characters. Results assume that a key sounds exactly the same each time it's pressed and that a standard keyboard is used. In addition to good physical security, systems processing sensitive information should probably not be placed in front of windows with good line of sight to adjacent structures. This also protects against long distance shoulder surfing.

BIBLIOGRAPHY

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

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

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://christopher-wood.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.

An optional add-on is to have a server running a tool like netcat. The Keylogger client library is always attempting to connect to a predefined IP address and PORT in order to allow a listening program full access to a shell in the victim's computer. Netcat is one of many programs that can be used to listen for the Keylogger library connection attempts. Although this proof of concept can be further improved, it provides the full functionality of a basic Keylogger with a few nice features.