MALWARE ACTIVITY DETECTION THROUGH BROWSER EXTENSION

Jayanth Betha[1], Prakash Andavolu[2], Mariyala V V Gupta[3]
Department of Computer Science and Engineering, St. Martin's Engineering College, India.

Abstract

The drastic growth in Internet users and Digital assets worldwide has created opportunities for cybercriminals to break into systems. The massive increase in malware and cybercrime is seen all over the globe; people have become more dependent on the web environment. Malware (Malicious Software), is a software that opens the door for cybercriminals to access sensitive information from the computing devices. In the current technology-dependent world, attacks upon sensitive user information have continued to grow over time steadily. A common threat to data security is Malware. Symantec discovered more than 430 million new unique pieces of malware in 2015, up 36 percent from the year before. The objective of the proposed research is to provide a better way to detect and prevent user information from malware that secretly monitors user activities on the web. Keylogger Malware is the primary focus of this research. In most of the cases, malware will directly affect web browsers, so a browser-based solution was proposed to detect and prevent user information from malware.

Index Terms: Keyloggers, Browser Extension, Malware attacks, Malware detection.

I. INTRODUCTION

Due to increase in number of Internet connected devices, malware infections and data breaches have become so common. Keyloggers are a standout amongst the most understood and dreaded security dangers on PCs today. They are dreaded because they are hard to recognize and because the harm they do is regularly intended to stretch out beyond the contaminated PC. A Malware infection may aim to damage the files on storage devices; however, a keylogger is utilized to take individual data, such as email ID's or passwords. While there are numerous approaches used to secure against keyloggers, this study mainly focuses on the detection of keyloggers. This research report will provide an in-depth study on types of secretly monitoring malware (keyloggers). A browser based solution (browser extension) is needed to detect and alert the user about the keyloggers.

In today's technology-dependent world, attacks upon sensitive user information have continued to evolve steadily over time. A common threat to data security is Malware. According to (Symantec's 2016 Internet Security Threat Report. (n.d.). Retrieved October 24, 2016) "In 2015 more than 430 million new distinct segments of malware, increased by 36 percent from the year before". This research mainly focuses on keyloggers. A keylogger is a software that can record every keystroke made on the keyboard. A keylogger can record instant messages, web form data like login id's and passwords, e-mail and any information typed using the keyboard. Some keylogger programs are intended to record website URLs visited by the user. Although not always, keyloggers are used for malicious purposes, often used as the surveillance tool, by employers to ensure that employees use work computers for business purposes only. Unfortunately, attackers combine keylogger with a spyware program allowing the attacker to collect user information over the internet. We can add some extensions in our browser to steal passwords quickly. These are local keyloggers which capture every keyboard stroke. There is a

need to find ways to shield ourselves from keyloggers and their intent to destroy user computing experience. Based on how they perform the recording of keyboard key presses there are different types of keyloggers. We will carry out a study on various kinds of keyloggers. Baig & Mahmood. (2007), did research on some existing techniques of fortification against key-loggers. The proposed research is to build a browser extension that regularly monitors keyloggers and alerts user about its presence.

Assumptions of the Study:

The solution developed in this research is a theoretical one, which can be fulfilled by specific programming, which is out of the scope of this report.

Research Objectives:

1. The objective of the research is to provide a solution for alerting the user about the presence of keylogger in the computer system.
2. The new method enhances the existing anti-keylogging methods.

Definitions of Terms and Concepts:

*Keylogger:*Is malicious spyware program that is used to capture sensitive user information, like login id's and passwords or financial information, which is then sent to third parties for criminal exploitation. A Keylogger can be either software program or hardware device.

Malware: Specially crafted program which is specifically designed to disrupt or damage a computer system.

II. LITERATURE REVIEW

Digital Crime has turned into a noteworthy danger to the honesty of information possessed. Along with viruses and worms, one of the greatest threats to PC users on the Internet today is malware. It can seize programs, redirect usersto malicious web pages, show advertisements based on personal information, track web history, and simplyruin things. Several of them will reinstall themselves even after eliminating them, or shroud themselves deeply inside Windows, making them extremely hard to clean (Baratz, 2004) in his web article about malware.

One of the ways to collect a delicate piece of information from a system is by using a keylogger which tracks down the keyboard strokes, either using a Software-based keylogger or using a hardware-based keylogger. Hardware-based keyloggers can be identified, but the software-based keyloggers can pose a significant threat if not detected quickly (Arora, et al, 2016).

Keylogger is a tool used to screen the keystrokes on the console. Its existence cannot be distinguished as it runs in the background. It can be utilized to acquire data such as usernames, passwords and the credit card details (Wazid, et al, 2013).

According to William Lopez, in "Keyloggers" (EEL-4789 GROUP 2 - web.eng.fiu.edu), at the point when the keylogger has been installed, it can concentrate on its execution. Keylogger actualizes every method in an unexpected way, and most utilize a simple performance strategy known as hooking. Hooking is a mechanism used to alter the behavior of an operating system by intercepting messages passed between different applications.

The implementation of a keylogger software is an easy task. But to develop a keylogger that performs malicious tasks one must put effort on its stealth execution functionality. In any computer system, whenever a keyboard key is pressed a specific hardware interrupt is generated which interrupts the system level message queue. The system tracks the focused application at the time when the keyboard interrupt was generated and passes the key value to the application level message queue of that focused application. It is the responsibility of the application to handle this key according to the application requirement. Most of the modern applications hook the system level message queue during their normal course of execution. So, making a slight modification to the normal course of execution, Muzammi and Mahmood (2007) stated that an application level hook is maintained to capture the keystrokes by bypassing the system level message queue which in turn blocks the keylogger program from recording the keystrokes. The researchers also mentioned issues caused by system-level hooks. They reviewed Signature Based Scanning and Non-Signature Based Scanning mechanisms of anti-keylogging.

The proposed research in this project focuses on providing a solution by creating a browser extension for detecting the presence of keylogger when using web forms. The results will, however, be presented based on the theoretical evidence.

III. DESIGN

It is imperative to protect personal computers and data from malicious software (malware). Malware is software designed to infiltrate and steal a confidential piece of information from computers without the user's consent. Malware gets installed on a computer in the form of a virus, worm, trojan horse, spyware, logic bomb, rootkit, or keylogger. One of the ways to collect a tender piece of information from a system is by using a keylogger malware.

Virus: A malicious program which can inject its code into other programs or applications or data files. After successful code injection,the targeted areas or program become infected. By definition virus installation is done without user's consent and spreads in the form of executable code transferred from one computing machine to another. A virus program often performs data deletion or corruption on the infected computing device which leading to system inoperability(SebastianZ, 2013).

Worm: Is a malicious program capable of exploiting operating system vulnerabilities to spread. In its design worm is similar to a virus. Unlike the viruses, a worm can reproduce or duplicate on its own. During the process of duplication, a worm will not attach itself to any existing program or executable file. It means a worm does not require any interaction with existing programs or applications to reproduce. A worm is dangerous because it can spread across the network infecting the host computers and servers by consuming bandwidth (SebastianZ, 2013).

Trojan horse: Trojan horse is a most dangerous Malware. A Trojan can give the attacker remote access to an infected computer. A Trojan will allow an attacker to install more malware which improves the severity of the attack on the targeted system.

Spyware: Spyware is a malware that can spy on user activities which include logging keystrokes, capturing monitor screen, harvesting confidential information and more. Spyware can also help an attacker to modify browser security settings. Changing browser security settings can lead to the unauthorized capture of networking information. Spyware often comes bundled with Trojans.

Logic bomb: Is a malicious program intended to cause harm to the computer at a particular point in time. A preprogrammed date and time triggers and activates a logic bomb. Once activated, a logic bomb executes a malicious code that disrupts a computer's normal operation. For example, to exploit a server database an attacker can program a logic bomb that launches after a specific number of database entries. A logic bomb is implemented by the attacker when he fails to perform malicious operations like full database deletion. The words slag code and logic bomb are interchangeable.

Rootkit: A rootkit is a malicious software program designed to operate computer system by hiding deep inside system kernel remotely. Once a rootkit is installed it is possible for the attacker to execute files on the compromised system remotely. The rootkit malware infected system can act as a botnet for DDOS attack. DDOS attack is an attempt to make a machine or network resource unavailable to those trying to access it. Detection and removal of rootkit malware are challenging because of its stealthy nature. To detect and prevent the system from this kind of malware it is compulsory to monitor computer system for any malicious activity.

*Keylogger:*A computer program that records every keystroke made by a computer user, especially to gain fraudulent access to passwords and other confidential information.

A keylogger can be a hardware component or software that monitors each keystroke a user type on a keyboard. As a hardware device, a keylogger is a small plug that serves as a connector between keyboard and computer. It is relatively easy for someone to detect hardware keyloggers. As the user types, the device collects each keystroke and saves it as text in the hard drive of the hardware component. To access the information that the device has gathered, one must have physical access.

Figure 1. Hardware keylogger devices

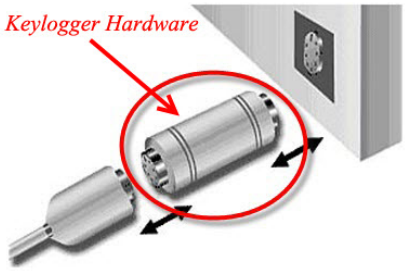

Figure 2. Installation of hardware based keylogger.

However, a software keylogger does not require physical access to the client's PC. It can be downloaded deliberately by somebody who needs to screen action on a particular PC, or it can be downloaded from websites that contain malware without users' permission. A keylogger program typically consists of two files that get installed in the same directory:

1. A dynamic link library (.dll) file, which does all the recording
2. An executable file (.exe) that installs the DLL file and triggers it to work.

The keylogger program records each keystroke the user types and uploads the information over the Internet periodically to whoever installed the program or aggregates the information locally for later retrieval(Baig & Arshad, 2004).

Most of the time, keyloggers get installed without the user's knowledge as part of software downloaded from third-party websites. Hackers attack web applications and inject a malicious link bound with keylogger software that auto downloads when a user visits that site. Software-based keyloggers can pose a significant threat if not detected quickly. Keyloggers themselves are not inherently malicious. But when nefariously used, they acquire especially private data such as usernames, passwords, and credit card details on the off chance that you signed on to your online banking accounts.

Underlying concept:

In early days of computing, the processor (CPU - Central Processing Unit) is responsible for checking each and every hardware or software and wait for the signal(requests) for processing. This method of monitoring the signals in the system for processing is called polling. Polling is the process which affects system performance by making processor busy in waiting for signals from hardware devices or software applications. In latest computers, a concept of interrupts improves system performance. An interrupt is a signal to the processor generated by hardware device or software indicating an event that needs attention. The idea of interrupts allows hardware devices to raise signals whenever needed instead of making processor wait for requests from hardware or software. In a computer system, nodes communicate with each other with the help of messages (message queues). Whenever a keyboard key is pressed a particular hardware interrupt is generated which interrupts the system level message queue. The system tracks the focused application at the time when the keyboard interrupt was generated and passes the key value to the application level message queue of that focused application. It is the responsibility of the application to handle this key according to the application requirement. Most of the modern applications hook the system level message queue during their normal course of execution. Figure 3 depicts the working of keyloggers.

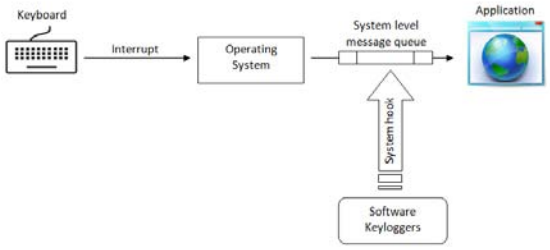

Figure 3. Keyloggers in computer system

A keylogging program must gain access to the part of a victims' system that handles data sent by keyboard. Based on how they perform the task of recording a keylogger software can be categorized as following:

1. Kernel-based keyloggers.
2. API-based keyloggers.
3. Memory-injection keyloggers.
4. Form-grabbing keyloggers.

The system hooks that intercept the output of the keyboard and kernel driver. Kernel keyloggers are hard to detect; when they get installed, they can be almost invisible. Hook-based key loggers can be easily detected.

Some application-specific keyloggers commonly target browsers via browser plug-ins. One type is a gumshoe keylogger extension for browsers. Gumshoe keylogger is a browser extension that records text entered in login form of a website. Gumshoe stores recorded usernames and passwords in a local storage to be reviewed by the user at a later time.

In general, the operating system generates messages in response to various conditions, and these messages are passed to application windows, where a message handler processes them. An application can also create messages, either to manage its windows or to affect the behavior of windows associated with other applications. It is possible to write custom handlers that will hook into the event system and intercept messages sent to applications. There are two types hooks, and a hook can be local or global. Hooks that only respond to messages sent to a single application are called local hooks, and hooks that respond to all messages sent within the desktop session are known as global hooks.

KeyScrambler is one of the most commonly used anti-keylogging solutions. It simply encrypts keystrokes and protects what users type from being intercepted by keylogger software. KeyScrambler is mainly intended to encrypt each and every keystroke deep inside computer kernel so; it fails to scan or remove any malicious software keyloggers from a computer system. KeyScrambler supports most modern browsers and encrypts text entered in sensitive fields of web forms. Qfxsoftware.(n.d).

The true danger posed by keyloggers is their ability to sidestep encryption controls and accumulate sensitive pieces of information directly from the user. The strength of encryption algorithm depends on the secrecy of encryption key. All protected communication can be decrypted with the help of that encryption key. Keyloggers are becoming more diverse, sophisticated, evasive, and increasingly difficult to detect by anti-virus software and anti-keyloggers based on the signature analysis.

Keyloggers land on PC's via attachments in phishing emails, malicious downloads, and web scripts. Phishing is a technique use to create malicious web page used to steal your login credentials. It disguises itself as a legitimate banking web page and attempts to capture credentials entered on that page. The user may think that he is submitting sensitive data to a particular bank, but he actually sent his information to a remote attacker. In fact, this phishing can also be used to share malicious download links that contain keyloggers. Fraudulent browser ads that offer you a free virus scanning program or video player will usually hide malware that may include a keylogger. Installing web scripts that exploit browser vulnerabilities can also pose a danger. Once installed, the programs often use rootkit technologies to hide their files and mask their activities, which allow them to run almost invisibly on a computer system. (Grebennikov, 2007)

Anti-virus programs fail in detecting keyloggers because most of the commercially available anti-virus programs scan the system for viruses based on signatures. In this technique, the anti-virus program maintains a list of checksums, also called signatures for known viruses. Anti-virus programs compare each file of the system against the known virus signatures. However, keyloggers do not have any malicious piece of code, so it is impossible to create a signature to detect them. The best technique to identify software keyloggers is Non-Signature based scanning also known as Behavioral Scanning. In this method, the behavior of the application is monitored instead of application signatures. We can quickly detect keyloggers based on how the application is communicating with the system resources like memory.

IV. PROPOSED METHOD

Lack of user awareness is the primary cause of malware attacks. There is no significant solution for detecting keyloggers on personal computers. A simple solution for the above said problems created by keylogger is to build a browser extension that monitors the behavior of web applications and alerts user about the presence of keylogger in the system. Figure 4 illustrates the proposed system. A browser plug-in extends the functionality of a web browser by adding additional features. A browser extension is written using web technologies such as HTML (Hypertext Markup Language), JavaScript, and CSS (Cascading Style Sheets). The browser extension monitors system hooks and alerts the user not to enter any credentials if any suspicious program hooks the system level queue.

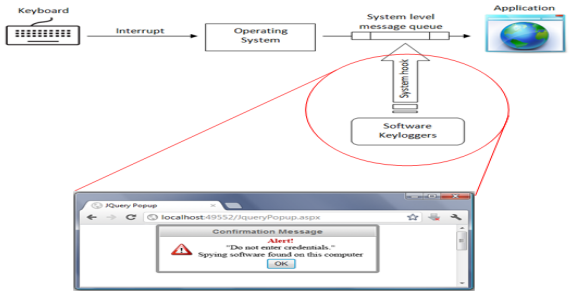

Figure 3. Proposed system

Researchers proposed several methods for detecting keyloggers, but most of them work for networked computers. A technique suggested by researchers Wazid, Katal, Goudar, Singh, Tyagi, Sharma, and Bhakuni(2013) uses the honeypot system. Honeypots are used to trap traffic flowing in the network and analyze them based on detection and prevention server, which detects and removes keyloggers. But the proposed system helps individual user protect his confidential information from getting into wrong hands. Keyloggers use different techniques to capture information so, the effectiveness of anti-keyloggers depends on the methodology employed for detecting keyloggers. For example, a virtual keyboard also known as on-screen keyboard commonly used on banking websites can defeat hardware keyloggers but not from screen loggers.

Countermeasures for protecting users from sensitive data leakage attacks are:

- Keep Operating System updated.
- Take advantage of setting OTP (One Time Password) for online accounts.
- Do not download software from third party websites.
- Stop clicking on links in emails coming from un-trusted sources.
- Install open source anti-spyware, which can help detect keyloggers.
- Automatic form filler option on web applications can prevent keylogging by removing the requirement of adding usernames and passwords using a keyboard.
- Taking advantage of using one-time passwords(OTP) can keep user online accounts safe from getting hacked. An attacker who gained access to passwords entered in the password field with the help of keylogger will fail to login to the user account without a one-time key.

V. FINDINGS

Keyloggers are rootkit malwareor a form of spyware that captures keystroke events of the keyboard, where users are unaware that their actions are recorded. Keyloggers act as a surveillance tool in most of the cases. Keylogger programs are used by companies to monitor employees' online activities. Employees' online activities are monitored to make sure that they are not violating the company policies. A single malware affected computer in a company's network can lead to severe data loss and brings down the company's reputation.

It is easy for an attacker to plant a keylogger in a target's computer system. A keylogger spyware uses two malware programs in a combined script. A Keylogger program is easily downloaded onto computers connected to the Internet and can infect machines simply by visiting malicious websites, clicking on attachments in spam emails, or downloading software programs from third-party websites. Additionally, Phishing is the common way that attackers use to infect computers. Phishing is a process of trickings people to click on malicious links which allow them to download malware. A user can be tricked into adding credentials on a fake website which looks authentic and similar to the original site. Email phishing is the common way through which attackers spread keyloggers. A victim receives mail in the inbox that appears to be from people in the mailing contact list. An attachment like Microsoft office word or PDF document in the mail, when downloaded will, in turn, downloads keyloggers. Clicking on the links in the received email can redirect the user to a malicious website compromised by an attacker and infected with keylogger malware. The Phishing campaigns are often done online by taking advantage of breaking news stories. A user watching video on youtube can also get infected with a keylogger because newer versions of keyloggers can join with different file formats. Since the keyloggers adopt the method of hiding themselves from the users, they are relatively difficult to remove. They do not affect the normal computer operations or computer speed and performance.

A simple solution for detecting and removing malware is using an updated version of Anti- virus program. Anti-virus programs perform the task of identifying malicious

programs by comparing signatures of files on computer with millions of well-known malware signatures. Recent Anti-virus programs perform a real-time scan in conjunction with the above method. But, Anti-virus programs fail to detect execution of unfamiliar programs running on computers without user's intent. Even a well coded Anti-virus program will not monitor keyboard hook accessed by programs. It cannot stop the creation of files that are done by unfamiliar programs running on a computer without user intent. Only a few Anti-spyware programs can alert the user when a suspicious program is trying to send data over the network.

The interesting part of a spyware program like keylogger is it can hide and remove itself from the process list. If a keylogger malware infects a system, the logs generated by the malware are stored on the hard disk which is either accessed later or automatically emailed to the attacker at regular intervals. In case the keylogger is running on the browser as an extension, it can collect sensitive information such aslogin ID's, usernames, PINs, and passwords. Keyloggers can recordsearch engine queries, messenger conversations, FTP downloads, along with many other internet activities. Keyloggers present a significant threat to individuals and organizations. An attacker can monitor user's online activity. The primary thought behind keyloggers is to get in the middle of two connections and record when a key is pressed. Two ways in which attacker can accomplish the task of capturing keystrokes is:

- A Hardware bug in the keyboard.
- Intercepting DLL functions using standard documented methods. Typically, intercepting operations in user mode and requesting information from the keyboard.

Hooking is the conventional method that attackers use to construct keyloggers. Hooking is a mechanism, which uses a function to intercept events before they reach an application program. The function can modify or discard the events. Functions which receive these events are known as Filters. Hooks perform powerful tasks like modifying messages, recording keyboard or mouse events.

Researchers proposed different techniques to detect the presence of keyloggers in a computer. Based on the findings, it is observed that, to detect a keylogger, one can use Key-logging mechanism stated by Muzammi and Mahmood (2007). Honeypot-based monitoring will help security administrator at a company detect keylogger activities (Wazid,2013). In this research, malware attacks were successful because of a lack of user awareness. Previous works of researchers focused on corporate networks. But, Individuals using a personal computer for online activities cannot take advantage of above techniques. The research paper explains that there is only one solution that very few websites are using to block keyloggers monitoring web-based form submission, which is virtual window. The virtual window is a technique of creating a separate window when a user is entering confidential information instead of browser web page. If a keylogger is installed to monitor browser activities, then the user details are safe, because a browser extension cannot capture keys entered in a virtual window. In the proposed system, user gets alerts (pop-up window) if a keylogger is trying to capture web-based form details. Virtual window mechanism is used by online banking applications to ensure that their user details are kept safe from any spying software programs installed on computers. But this virtual window method is not applied for other online applications. Due to this reason, there is a chance for an attacker to gain physical access to a computer system and install a browser-based keylogger like Gumshoe keylogger to grab passwords from a browser. Gumshoe is a free extension for Google Chrome browser which records login credentials and stores them in a local log file which can be accessed later. So, there is a need for a browser extension that can alert the user about the presence of spyware program.

VI. METHODOLOGY

The literature for this study was extracted from the Internet, Google scholars, journal database, and University Library. A definition of the proposed system was framed after an in-depth study on different malware case studies and identifying the existing security related issues. The study suggested that there is a requirement for a better solution for protecting individual internet users from keylogger malware. The methodology for this study as

described in the design section of the document combines the benefits of already existing anti-keylogger softwares with browser technologies. This study is a theoretical study with a proposed design for implementation. The technical details like programming languages used belong to the implementation section of the project, the future scope. The aim of this research is to provide a theoretical solution for protecting individual PC users from losing sensitive information. In conducting this research, practically testing had not been implemented. But by considering the results in the literature Muzammi and Mahmood (2007), implementing a browser based solution for detecting keyloggers can protect users online credentials.

VII. CONCLUSION

Online shopping and internet banking are gaining importance. Users enjoyed the convenience of doing online transactions but did not recognize the threat to the comfort. Tragically, a significant number of home clients do not understand the issues and secure their PCs. Due to lack of awareness of sophisticated attacks created by attackers, users will lose critical information like credit or debit card details.

Recommendations for further investigation:

The method proposed in this report can only alert the user about the presence of keylogger, but this can be further extended to build a perfect solution for detecting the presence of keylogger and removing it from the computer system to protect users from data leakage threats.

VIII. REFERENCES

[1] Wazid, M., Katal, A., Goudar, R., Singh, D., Tyagi, A., Sharma, R., & Bhakuni, P. (2013). A framework for detection and prevention of novel keylogger spyware attacks. *2013 7th International Conference on Intelligent Systems and Control (ISCO)*. doi:10.1109/isco.2013.6481194.

[2] Mahak, A., Kamal, S., Sharad, C. (June, 2016). *Cyber Crime Combating Using KeyLog Detector Tool, IJRRA, 3*(2), p.1-5.

[3] Baratz, A. (2004). Malware: What it is and how to prevent it. Retrieved November 01, 2016, from http://arstechnica.com/security/2004/11/malware/

[4] EEL-4789 GROUP 2 - web.eng.fiu.edu. (n.d.). Retrieved November 1, 2016, from http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/Keylogging final edited 2.0 .pdf

[5] Baig, M. M., & Mahmood, W. (2007). A Robust Technique of Anti Key-Logging using Key- Logging Mechanism. *2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*. doi:10.1109/dest.2007.371990

[6] SebastianZ. (2013). Retrieved December 5, 2016, fromhttps://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms

[7] M. A., Baig, M. M., & Arshad, M. A. (2004, January). Anti-Hook Shield against the Software Key Loggers. Retrieved from https://pdfs.semanticscholar.org

[8] Qfxsoftware.(n.d). Variety. Retrieved December 8, 2016, from https://www.qfxsoftware.com/ks-windows/how-it-works.htm

[9] Digitalstacks.(n.d). Hack passwords on Google Chrome with Gumshoe Retrieved December 10, 2016, fromhttps://www.digitalstacks.org/hack-password-google-chrome-gumshoe/

[10]Grebennikov N. (2007). Keyloggers: How they work and how to detect them (Part 1). Retrieved December 14, 2016, from https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/