KeyStroke Logs: Are Strong Passwords Enough?

Darshanie Sukhram Thaier Hayajneh
Fordham Center for Cybersecurity
Fordham University
New York NY USA
{dsukhram1, thayajneh}@fordham.edu

ABSTRACT

As hackers develop sophisticated phishing and social engineering attacks, it is recommended that users be aware of common tactics and implement stronger and unique passwords for sensitive accounts. Malware typically involved in cyber-attacks includes viruses and worms. Keyloggers are designed to track and capture keystrokes made on devices. They are not given the same priority as the other types of malware, but are also considered malicious as it poses the same level of risk. Having a strong password in this instance does not provide a high level of protection as keyloggers will log each key typed. This paper will discuss the characteristics of keylogging software while providing a summary on methods of protection. Three keylogging software are tested against two anti-keylogging programs to identify what information is captured and which method of protection is stronger. A discussion on risk assessment with regards to keyloggers and remediation techniques is also included.

Key Terms: Keylogger, Anti-keylogging software

I. INTRODUCTION

Keyloggers are used to monitor and track keystrokes made on computers. It allows social engineering to be relatively simple as hackers can identify the operating system, username, specific log on times, and system information of a particular device. Based on these attributes, a hacker can search for known vulnerabilities that could be used to exploit the target system [10]. If the same aspect of the system is compromised repeatedly, it can be inferred that there is either insufficient patching or that new vulnerabilities are consistently being developed.

Once the target is specified, the hackers try to gain access using social engineering techniques. For a hacker to compromise a system, they first need to gain access to the network or target system. A combination of brute force or dictionary attacks could be used to grant access to a locked account [2]. Phishing emails based on reconnaissance methods could also provide necessary credentials, however keyloggers relieves hackers from using traditional reconnaissance techniques. Using keyloggers in malicious attacks are just as effective as implementing common malware such as viruses and worms [9]. It allows passwords and usernames to be exposed without much effort as with hacking servers for these same attributes [11].

In the early history of keyloggers, they were widely used in e-commerce as hackers would use the software to capture financial information from consumers when they made purchases online. Credit cards, billing information, and account credentials were logged, in addition to critical banking information. Traditional keylogging software was limited to only logging keys that were being physically pressed on the keyboards, but modern programs include the keys touched or clicked on using virtual keyboards that are located onscreen. As the use of keyloggers evolved, hackers can also obtain screenshots of user desktops and export the logs of keystrokes generated [10]. Rather than export through email, logs and other network traffic captured can be exported through stealthy methods using backdoors and reverse shells [1]. These stealthy methods may bypass firewall rules depending on how the network is designed.

Some ways to defend against keyloggers is by implementing web proxies to filter data captured, specifying access control policies, and by installing keylogger detection software such as antivirus programs [11]. Password managers can also prevent keystrokes from being captured as users are not required to type each individual password for every

978-1-5386-1104-3/17/$31.00 ©2017 IEEE

account [7]. Increasing user awareness about the consequences of keyloggers may urge them in using stronger passwords and implementing password managers to better protect their assets.

Keyloggers can be applied from an ethical perspective as well. Noting the way in which a particular user types can be integrated as a biometric defense in protecting or validating an authorized user [3]. Monitoring keystrokes for young children and particular users may also be beneficial in ensuring the sites they are viewing are appropriate [4].

The following components of this paper are as follows. Section II discusses the functionality of keylogging programs, both from an ethical and unethical standpoint. It includes an overview of the related work found in literature. Although the focus of this paper is on unethical uses, keylogging software can be used to authenticate and validate users. Section III demonstrates the impact of selfish behavior on network performance. An experiment including three distinct keyloggers was conducted to identify types of logs generated and information captured based on user data. These programs were individually tested two additional times, each with the installation of one anti-keylogging software and one anti-virus software. Details on how the keyloggers were identified are also included. Section IV relates the impact of keyloggers as a notion to bring awareness to the importance of risk assessment in creating a validated security posture. Section V provides recommendations on how to protect against keyloggers. Finally, Section VI highlights the overview of this paper.

II. Functionality of Keyloggers

Keyboards have open circuits under each individual key and when any given key is pressed, that circuit is closed to make the connection. When pressed, the circuit location is mapped to a table in the keyboard ROM to identify which letter, number, or symbol was identified. This information is stored temporarily and is sent to the operating system to display the information on screen [11].

The keyboard includes three layers of plastic that work together to create a switch effect so that when a key is pressed, a connection is established instantaneously. The upper and lower layers are covered in electrically conducting metal tracks with an insulation layer in the middle. The lower layer encompasses electrical connections that bridge the circuit when the upper layer makes contact.

Keyloggers monitor the keystrokes made and store the results in various logs. Some are more complex as they track applications accessed and capture screenshots of what is displayed on user machines [4].

There are generally two main types of keyloggers which include software and hardware. Software based keyloggers capture keystrokes as it passes between the operating system and the keyboard interface. Hardware keyloggers refer to a physical piece of equipment that is plugged in between the keyboard and the computer. This piece of equipment encompasses a processor that writes the keys pressed to its own internal memory processing unit. No files are logged or identified on the target machine [11].

From an ethical standpoint, keyloggers can be used as a method of identification. Monitoring the way in which a user types with references to speed and force of touch, keyloggers can be used to study the behavioral biometric of typing. Each individual follows a unique typing rhythm that is based on the timing of each key as it is pressed and released. These minuscule measurements can be analyzed similarly to the way eye movements are studied as a means of validating identification. There are differences in the way a user types for word processing, spreadsheet typing, and web browsing. [3]. Rather than implementing a password that can be uncovered by keyloggers, devices can grant access by confirming the typing metric of an individual user.

Keyloggers can also be implemented as parental controls to monitor sites and applications used by young children [4]. From a cyber security perspective, it can help in incident response handling by reviewing the actions of potential suspects during an investigation.

From an unethical standpoint, keyloggers can be used to extract credentials entered on a system in a malicious manner. Some keylogging software run in the background of an operating system and is not seen by the end user. It sits in the background but actively records each key that is pressed. In some instances, keyloggers are also hidden from task manager and list of operating processes [4]. It may also be referred to as spyware as it gathers information without the user

Table 1: Results of keyloggers tested

	Phrozen Key Logger Lite	Actual Key Logger	Refog Free Key Logger
Logged Keystrokes	✓		✓
Logged Keystrokes made within Browser			
Captured Screenshots		✓	✓
Screenshots Visible		✓	
Tracks Applications Used	✓	✓	✓
Keystrokes Visible in Plaintext	✓		✓
Hot Key Combination	✓	✓	✓
Special Password	✓		

knowing [5]. Hackers may also take advantage of click tracking software to assist with keyloggers.

The click tracking software monitors mouse clicks on a system. Hackers can obtain a detailed history of what applications were accessed, which links were clicked, and then reference the keystrokes to identify which credentials match the sites or applications accessed [6]. Websites such as Google, Bing, and Yahoo tracks user clicks for marketing purposes automatically, so it would be simple for hackers to reference this information after installing keylogging software.

III. Keylogging and Anti-Keylogging Testing

For the purpose of this paper, three open source keylogging software were tested to identify what information could be captured. This experiment was conducted using a Windows 7 Virtual Machine and was repeated three different times to verify the results. Table 1 below shows the results from the first test instance. Details of all three test instances are described in the following paragraphs.

Table 2 displays information based on two open source anti-keylogging software that were also tried, one specific anti-keylogging program and one general anti-virus program that had anti-keylogging functionalities. SpyShelter is the anti-keylogging specific software while Malwarebytes Anti-Malware is the generic anti-virus software. There was other software initially chosen to be tested, however there were issues with the installation and verification processes. The final five software used are identified in the tables below.

Table 2: Results of preventive software tested

	SpyShelter	MalwareBytes Anti-Malware
Identified Phrozen Key Logger Lite	✓	
Identified Actual Key Logger	✓	✓
Identified Refog Free Key Logger	✓	✓
Alerted User on Key Logger Identified	✓	
Deleted Key Logger Software Identified		✓

A. Phrozen Keylogger Lite

Phrozen Keylogger Lite 1.0 was the first keylogger to be tested. Once the installation process was completed, it asked for a password and a command to be specified. This credential and hot key combination enables the user to access the software as needed. The icon created on the desktop and the icon within the programs menu does not launch the software as the command created is the only way to open the software. When prompted, the user enters the password. When entered correctly, the user sees a list of applications logged based on time and date opened. When an application session is chosen, a window pops up that displays the keystrokes made on that application.

The first testing of this software did not display text entered within the browser. For example, when typing in credentials for a web based email account, Phrozen Keylogger Lite only displayed that the email website was accessed. However, when text was entered in the URL or within a text document, those keystrokes were recorded. Additionally, this software did not capture any information about screenshots that were taken.

With regards to the anti-logging software, SpyShelter Firewall notified the user that Phrozen Keylogger Lite was installed on the computer and was malicious. In attempts to uninstall the keylogging software, it was not listed under Uninstall Programs within the Control Panel in Windows. This made it difficult to remove the keylogging software. The folder within the directory also did not provide an option to uninstall the software. Deleting the shortcut and icon from the desktop and program menu did not uninstall the software; it was still accessible using the hot key combination.

After SpyShelter Firewall was installed, a popup displayed that Phrozen Keylogger Lite was trying to monitor clipboard changes. It included the file path of that software to show the user where the malicious content was located. When ignoring the warnings to type in a text document and on the web, all keystrokes logged were now hashed. Instead of a plaintext view of the keystrokes, there were strings of numbers that represented each typed word. Again, no text within a given web page was logged. If a hacker were to decrypt the hash, they would still be able to view the logs in plaintext. When SpyShelter Firewall was uninstalled, Phrozen Keylogger Lite reverted back to capturing keystrokes and displaying them in plaintext to the user. No other characteristics were affected.

The next testing examined how Phrozen Keylogger Lite worked in response to Malwarebytes Anti-Malware 2017. No popups were given to warn the user of this malicious software. After scanning the machine, Phrozen Keylogger Lite was still not identified by this anti-keylogging program. The keystrokes captured was still visible in plaintext as without any anti-keylogging software installed, however text entered within the browser could now be detected. For example, the credentials entered on a web based email account was now captured in the keystroke logs on the Phrozen Keylogger Lite software.

B. Actual Keylogger

The second keylogging software tested was Actual Keylogger. This open source program captures more information than Phrozen Keylogger Lite and provides a cleaner menu for user experience. It shows a list of applications used with their given file paths. The username for the computer is also noted on each log generated with the time and date. Actual Keylogger did not, however capture any keystrokes made on the virtual machine. Whether it be from a text document, browser, or web page, no keystrokes were recorded.

Aside from the applications accessed, a screenshot could be taken after specifying a particular time. The image captured could be accessed within the Actual Keylogger console to allow the user to see everything that was on the screen at that moment in time. When the screenshot is taken, the user sees no changes on the desktop itself. This provides a discrete method for hackers to see the screens of their given targets.

SpyShelter Firewall provided a popup alerting the user of the Actual Keylogger software. It cautions the user that the keylogging program is trying to take a screenshot of the display or window. There is another alert that describes the program trying to communicate with other processes when trying to take the screenshot. When SpyShelter Firewall is not installed, the user has no such warnings or indications that a screenshot is being taken.

Malwarebytes Anti-Malware also did not identify the Actual Keylogger software after completing a full scan on the machine. Given some activities on the machine, Actual Keylogger was opened again to identify any changes. When accessed, Malwarebytes Anti-Malware generated a popup to identify Actual Keylogger as a malicious program. A second scan was then executed which quarantined Actual Keylogger as malware. Once the second scan was complete, Actual Keylogger could no longer be opened. Malwarebytes Anti-Malware changed the file path and the software could not be accessed. Uninstalling and reinstalling the keylogging software to the same destination provided the same results; the file path could not be accessed and the software could not be opened. Reinstalling the program in a different location was, however, successful.

C. *Refog Free Keylogger*

The third software tested was Refog Free Keylogger. This application allows the user to specify the machine they want to monitor. It gives some standard options for a child, an employee, or personal computer. Regardless of which account is chosen, the interface divides the logs generated by username. It also allows a hot key combination to access the program discreetly. Unfortunately, this option did not work when tested.

The keystrokes captured did not include any text entered within websites, only what was typed in the browser URL. All other texts were recorded and was stored in plaintext. Refog Free Keylogger also kept track of applications used by each user and included an option to capture screenshots when specified. However, the application did not generate a preview when requested. Reinstalling the software a second time allowed the text entered in web pages to be recorded. For example, entering credentials for a web based email service was not accessible.

The one downside to Refog Free Keylogger is that the user must open the application and select the option of beginning the monitoring process for any activity to be logged. This is inefficient for hackers as they would not want the software to be displayed in plain sight.

With regards to SpyShelter Firewall, Refog Free Keylogger was immediately identified. The keylogging software could not install without giving proper permissions. Once the user allows the installation process and the process is completed, a popup shows the user that the application was trying to get texts of other applications. Continuous popups were generated, more so than with the other keylogging software tested. As one was closed, another would immediately open.

Malwarebytes Anti-Malware also identified Refog Free Keylogger. Once installed, a scan immediately began and the results showed that the malware was quarantined. When trying to access Refog Free Keylogger, the virtual machine crashed. Upon rebooting the system, Refog Free Keylogger and Actual Keylogger were deleted and removed automatically. Phrozen Keylogger Lite was still visible as the icon and shortcut remained, however the hot key combination was no longer working.

IV. RELATED WORKS

Cyber risk management must be performed for organizations to understand vulnerable areas with regards to their cyber security posture. They must examine critical assets and determine possible threats that may escalate into attacks and incidents. For a given asset, organizations need to ask the following questions. What would happen to the business functionality if this asset was compromised? Who will be affected? Will the brand reputation be damaged when faced with an incident? How would an attacker compromise this asset? How can the network be protected and alerted in the event of an intrusion? Who are the incident responders and how will they process an investigation?

When the risk assessment phase is complete and the questions above are answered in detail, corresponding controls which would mitigate the risk must then be designed. Drafting an incident response plan and identifying key responders would be the next step before implementing the controls on a live system.

Viruses, worms, and trojans are commonly thought of as malicious programs that can infiltrate a system to exploit sensitive areas and obtain critical information. Keyloggers are another form of malware that is not discussed as often as these common programs, although it poses the same risk if not higher risk for organizations and enterprises. These entities should keep in mind the consequences of keyloggers when assessing risk and designing controls. As seen with the software in the experiment, keyloggers can not only track keystrokes but also capture images of desktops and monitor applications accessed.

Moreover, in some cases users may lessen their security to keep the system's performance high [13, 14, 15, 26, 27] or use lightweight cryptography [28, 16, 17, 18]. It is also worth mentioning that some systems are vulnerable to attacks that cannot be prevented using cryptographic protocols, such as: jamming [19], MAC misbehaving [20], packet dropping [21], wormholes [22, 23] and localization [24, 25].

V. Recommendations

Password managers can relive what is known as password fatigue. Cybersecurity recommendations prefer having a strong password of about twelve characters, including a combination of numbers, symbols, and letters. These long passwords are often difficult to remember as some users may just write them down on a sticky note next to their monitor to recall their credentials. Despite keyloggers being able to track what is typed, leaving notes with passwords exposed causes high risk for stolen credentials. Password managers can help to remediate this risk by providing a secure location for various passwords [7, 8].

Users can create one master password for their password manager account and then log each credential for additional accounts within that one application. Browser extensions can be integrated for easy access depending on what sites are supported by each browser [8]. The master password and each cached password can have encryption protection as well. The master password can be used as the public key in the encryption process. This means that the passwords stored in the application, or wallet, are encrypted and can only be decrypted with the corresponding master key. This process of dual possession authentication is secure as one component is useless without the other [7].

Web attacks could also violate password managers that have extensions integrated in the browsers. A security control that can help to mitigate this risk is to have web proxies filtering trusted sources that are approved and authenticated. Browsers share cookies that can be exploited cross site if compromised in one particular instance [8].

Another recommendation would be to use two factor authentications. In the event that an account is compromised or the password manager is infiltrated, the hacker would not be able to use the credential without that secondary token. This would alert the user immediately of an unknown source of login as the notification for granting the secondary token will be pushed automatically when trying to log in.

VI. Conclusion

In addition to using password managers and two factor authentications, organizations and enterprises need to install validated anti-keylogging software. As the results in the experiment have shown, anti-keyloggers and anti-virus software focus on different aspects. An anti-keylogger such as SpyShelter focuses on alerting users on specific keylogging attributes while anti-virus software scans applications based on known malicious signatures. It is up to individual organizations to assess the risk they may encounter to determine the appropriate controls and prevention software to implement in their day to day operations.

References

[1] Anil Kurmus, Aurelien Francillon, Davide Balzarotti, Erik-Oliver Blass, and Jonas Zaddach. “Implementations and Implications of a Stealth Hard-Drive Backdoor.” Web.

[2] Apurva Pawar, Balaji Patil, and Hemita Pathak. "A Survey on Keylogger: A Malicious Attack." *Internation Journal of Advanced Research in Computer Engineering & Technology* 4.4. 2015. Web.

[3] Brian Tschinkel, Bernard Esantsi, Dominick Iacovelli, Padma Nagesar, Richard Walz, Vinnie Monaco, and Ned Bakelman. "Keylogger Keystroke Biometric System." *Research Gate*. 2017. Web.

[4] Charles E. Frank, Donald H. Galli, and Kishore Subramanyam. "Keyloggers: The Overlooked Threat to Computer Security." Web.

[5] Christofer Sean Cordes. "Monsters in the Closet: Spyware Awareness and Prevention." *Educause Quarterly*. Web.

[6] Cliff C. Zou, Erich Dondyk, and Roberto Alberdeston. "Click-tracking Blocker: Privacy Preservation by

Disabling Search Engines' Click-tracking." *2014 IEEE Global Communications Conference*. 2014. Web.

[7] Daniel McCarney, David Barrera, Jeremy Clark, Paul C. van Oorschot, and Sonia Chaisson. “Tapas: Design, Implementation, and Usability Evaluation of a Password Manager.” Web.

[8] Dawn Song, Devdatta Akhawe, Warren He, and Zhiwei Li. "The Emperor's New Password Manager: Security Analysis of Web-based Password Managers." Web.

[9] Evangelos Ladakis, Giorgos Vasiliadis, Sotiris Ioannidis Lazaros Koromilas, and Michalis Polychronakis. "You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger." Web.

[10] Mehdi Dadkha and Mohammad Davarpanah J Azi. "A Novel Approach to Deal with Keyloggers." *Oriental Journal of Computer Science & Technology* 7.1. 2014: 25-28. Web.

[11] Olzak, Tom. "Keystroke Logging (Keylogging)." *Encyclopedia of Social Media and Politics*. Web.

[12] Peter Nemcek. "Analysis of Malware Classification Schemas." Web.

[13] T. Hayajneh, S. Ullah, B. Mohd and K. Balagani, "An Enhanced WLAN Security System with FPGA Implementation for Multimedia Applications," IEEE Systems Journal, 2015.

[14] T. Hayajneh, B. Mohd, A. Itradat and A. Quttoum, "Performance and Information Security Evaluation with Firewalls," International Journal of Security and Its Applications, SERSC, vol. 7, no. 6, pp. 355-372, 2013.

[15] T. Hayajneh, S. Khasawneh, B. Mohd and A. Itradat, "Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications," in Proc. of The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2012.

[16] Bassam Jamil Mohd, Thaier Hayajneh, Khalil M. Ahmad Yousef, Zaid Abu Khalaf, Md Zakirul Alam Bhuiyan, Hardware design and modeling of lightweight block ciphers for secure communications, Future Generation Computer Systems, 2017, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2017.03.025.

[17] B. J. Mohd, T. Hayajneh, Z. AbuKhalaf, K. Yousef “Modeling and Optimization of the Lightweight HIGHT Block Cipher Design with FPGA Implementation,” Security and Communication Networks, John Wiley, Vol. 9, No. 13, pp 2200-2216, 2016. (DOI: 10.1002/sec.1479)

[18] BJ Mohd, T. Hayajneh, M. Z. Shakir, K. A. Qaraqe, AV Vasilakos “Energy Model for Light-Weight Block Ciphers for WBAN Applications,” In Proc. of IEEE 4th International Conference on Wireless Mobile Communication and Healthcare (IEEE MobiHealth'14), Athens, Greece, 2014.

[19] K. Panyim, T. Hayajneh, P. Krishnamurthy and D. D. Tipper, "On limited-range strategic/random jamming attacks in wireless ad hoc networks," in Proc. of IEEE Conference on Local Computer Networks (IEEE LCN), 2009.

[20] Hayajneh, Thaier, Ghada Almashaqbeh, and Sana Ullah. "A Green Approach for Selfish Misbehavior Detection in 802.11-Based Wireless Networks." Mobile Networks and Applications 20.5 (2015): 623-635.

[21] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Kim, T. Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6.

[22] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Le, A. Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies. Mobile Netw. Appl. 2012, 17, 415–430.

[23] Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks. In Proceedings of the IEEE 3rd International Conference on Network and System Security, Gold Coast, Australia, 19–21 October 2009; pp. 73–80.

[24] Hayajneh, T.; Doomun, R.; Krishnamurthy, P.; Tipper, D. Source—Destination obfuscation in wireless ad hoc networks. Secur. Commun. Netw. 2011, 4, 888–901.

[25] Doomun, R.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Secloud: Source and destination seclusion using clouds for wireless ad hoc networks. In Proceedings of the IEEE Symposium on Computers and Communications, Sousse, Tunisia, 5–8 July 2009; pp. 361–367.

[26] Bhuiyan, Md Zakirul Alam, et al. "Event Detection through Differential Pattern Mining in Cyber-Physical Systems." IEEE Transactions on Big Data (2017). (DOI: 10.1109/TBDATA.2017.2731838)

[27] T. Hayajneh, R. Doomun, G. Al-Mashaqbeh, BJ Mohd “An energy-efficient and security aware route selection protocol for wireless sensor networks,” Security and Communication Networks, John Wiley, Vol. 7, No. 11, pp 2015-2038, 2014. (DOI: 10.1002/sec.915)

[28] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, “A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues,” Journal of Network and Computer Applications, vol. 58, pp. 73–93, 2015.