ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
April 2014,
Vol. 7, No. (1):
Pgs. 25-28

A Novel Approach to Deal with Keyloggers

MEHDI DADKHAH, MOHAMMAD DAVARPANAH JAZI

[1]Master student, Department Of Computer and Information Technology, Foolad Institute of Technology, Foolad shahr, Isfahan 8491663763
[2]Faculty member, Department Of Computer and Information Technology, Foolad Institute of Technology, Foolad shahr, Isfahan 8491663763

(Received: March 24, 2014; Accepted: April 03, 2014)

ABSTRACT

Keyloggers have been widely used by hackers as a tool to steal information and passwords from users in e-commerce. The malware security software has also grown but keylogger grow too. This article reviews some of the techniques used by hackers to spread Keyloggers and bypass various security techniques by using advanced Keyloggers and finally, we describe a novel approach to deal with Keyloggers. This approach, capable of dealing with the most advanced Keyloggers, and greatly reduces damage caused by Keyloggers.

Key words: Keyloggers, malware, virtual keyboard, social engineering.

INTRODUCTION

Keyloggers are software programs that monitor user input data to gather information concerning these data and are often used with malicious intent. Data collected by Keyloggers usually contain personal and financial information such as bank account user name and password, email or text messages and etc[1]. Increased use of personal computers for financial and e-commerce transactions has fueled the growth of Keyloggers. Furthermore, the advancements in programming languages provide new powerful tools for attackers to develop more advanced types of Keyloggers to achieve their objectives.

Keyloggers Overview

There are many Keylogger types, but in general they can be classified in three categories: hardware, software, and web keyloggers. Hardware keyloggers are plugged in the hardware system, between the input devices and a computer[2]. Web keyloggers are web scripts written in Java and can often open an invisible pop-up window and collect user information. Also, it is possible to embed malicious code into vulnerable web sites to collect data entered by the user. In this article we will discuss Software Keyloggers and provide a framework to deal with them.

Existing methods for dealing with Keyloggers

The old Keyloggers had a clear structure. The key strokes of the keyboard itself were recorded and then sent by email or FTP to the attacker[1]. So to deal with it, the virtual keyboard was designed for electronic payment pages[3]. Each

time you log in to a financial portal, the place of button of keyboard change in virtual keyboard and attacker cannot understand which key is pressed; therefore Keylogger's maker will not be able to capture any passwords. Also, security software used by the operating systems, carefully examines the Startup to prevent Keyloggers from running concurrently with platforms at the same time. These applications were able to identify the new Keyloggers by checking Keyloggers files and verifying the structure of the executable[4].

New Techniques used in Keyloggers

Today's Keyloggers can record keyboard keys pressed by the keys on the virtual keyboard. Such Keyloggers receive consecutive screenshot from the victim's monitor, and can then identify strokes of the keys.

Also today's Keyloggers instead of running through the Startup, they run through Task scheduler (i.e. they run at a specific time and date, e.g. 5 minutes after loading the operating system), or as a Service in objects in which Antivirus software have less control over their actions.

Today's Keylogger's makers are capable to change its assembly by using specialized software after creating their Keylogger, so that it encapsulated. After encapsulating the Keylogger, a lot of security software will not have the ability to identify the new Keylogger. As part of the research carried out for this paper, a Comparison was performed on the results from 19 top security software applications in the world. Before the encapsulations, 8 software applications were able to identify the Keylogger. (Figure 1) After encapsulating the Keylogger in a series of successive operations, by changing the assembly to encode a string, majority of the security software failed to detect Keylogger and only two security applications were able to identify the Keylogger

Fig. 1: Number of identified 'non-encapsulated' Keyloggers by security software

Fig. 2: Number of identified 'encapsulated' Keyloggers by security software[1]

1. This test is done in Anubis and Jotti's lab. Jotti's malware scan is a free online service that enables user to scan suspicious files with several anti-virus programs. Scanners used are Linux versions; detection differences with Windows versions of the same scanners may occur due to implementation differences.

(Figure 2).Keylogger's maker now can easily embed Keyloggers acting on their own image or file. The attackers create a Keylogger file with an image, then write a few lines of code, and set the image to open the written programs. Keylogger can be merged then concurrently with the three files and output package is a final executable file that contains the encapsulated source, Keylogger files and image. Extension Spoofing loading procedure called a security hole in the Windows operating system that uses file extensions to any arbitrary extensions such as Mp3 and Jpg and selects an appropriate icon for that file extensions[5].

Another way in which attackers apply Keyloggers to infect their victims is JDB Keylogger. In fact, this type of Keyloggers is combination of Software Keylogger and Web Keylogger. In this approach, attacker created Java file on a website and written running code of the file in Java on the site. Anyone visit the site; Keylogger will taint his operation system[6].

Use of Social Engineering

The art of social engineering is to exploit vulnerabilities in human behavior to create a security breach without the victim's suspicious. Social engineering is misused to deceive people and to persuade them with different methods to get their information.

Instead of using invasive methods and the direct access through the firewall to access the organization's systems and databases, they track people who have access to the information and use social engineering techniques to influence them to gather the information they need[7].

Social engineering through computer systems is done in several ways:

- Pop-Up windows
- E-mail Attachments
- Deceptive spam and chain
- Websites
- Retrieval and Analysis Tools Used
- Phishing

Recently Keyloggers authors also use social engineering to achieve their goals.

Since Keylogger should be run on the victim's operating system, social engineering can be also efficient. Changing executable file's extension and changing its icon are samples of social engineering to trick the victims.

Since there are different operating systems requiring different executable files, social engineering tool are used to identify the type of victims' operating system and sometimes to identify the security tools used, which can make the attack more efficient.

Using social engineering tools attackers have not only a way to identify the operating system, but by taking advantage of tools and known exploits, it has also the ability to take advantage of the operating system's security vulnerabilities (e.g. Windows XP) and then run the Keylogger there[8].

Counter Keyloggers by Flash Keyboard

The approach proposed in this paper to deal with all types of Keyloggers is Flash Keyboard. By using existing capabilities of Adobe Flash files or Microsoft Silverlight, virtual keyboard online payment pages are designed to use animated mouse pointers on which they are moving. Thus getting a screenshot from virtual keyboard, attacker would not be able to determine which key has been pressed by the victim (images will be the same as in Figure 3) and it will be impossible to guess the password. Thus, even in situations where the computer system is already infected, the keylogger won't be able to steal passwords and

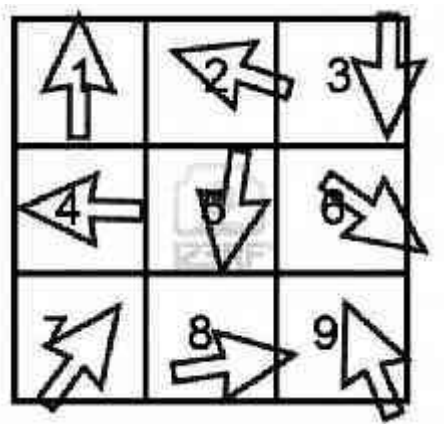

Fig. 3: Captured images of Flash Keyboard

user name. And since all passwords are entered by the virtual keyboard, from which Keyloggers cannot record any data, the captured by Keylogger screenshots will be vague too.

Conclusions and Recommendations

In this paper we have briefly introduced various Keyloggers types and techniques that are currently used to deal with them. Then with the introduction of advanced Keyloggers, we've shown the existing approaches to deal with keyloggers may fail. And finally, we've presented our new approach to deal with different types of advanced Keyloggers.

REFERENCES

1. Christopher A. Wood and Rajendra K. Raj," Keyloggers in Cybersecurity Education", New York, USA (2010).
2. Wikipedia., Hardware keylogger",online Document avalaible at: http://en.wikipedia.org/wiki/Hardware_keylogger (2014).
3. Afolayan A. Obiniyi and Mohammed Aminu Umar,"Random Number Based Dynamic Anti-Screenshot Virtual Keyboard for Securer Web Login", The International *Journal of Engineering And Science*, **2**: (2013).
4. McAfeeInc," McAfee Virus Scan Enterprise 8.8 Best Practices Guide", (2010).
5. Mehdi Chehel Amirani, Mohsen Toorani, Ali A. Beheshti," A New Approach to Content-based File Type Detection", IEEE (2008).
6. Oracle (March 2014), " jdb - The Java Debugger", online Document available at: http://docs.oracle.com/javase/7/docs/technotes/tools/windows/jdb.html
7. Christopher Hadnagy," Social Engineering: The Art of Human Hacking", Canada, Wiley Publishing (2010).
8. Metasploit project. [Online]. Available: http://www.metasploit.com