RESEARCH ARTICLE OPEN ACCESS

Keyloggers and its Demonstration

Gaurav Salvi[1], Sanket Khambal[2], Supriya Dicholkar[3]

Department of Electronics and Telecommunications Engineering,
Atharva College of Engineering Malad-Marve Road, Charkop Naka, Malad (West), Mumbai-95
University of Mumbai, India
gauravsalvi0104gmail.com,khambalsanket95@gmail.com, supriyadicholkar@atharvacoe.ac.in

Abstract:

In todays world, computers are used everywhere to carry out various important tasks.Due to this the security of these devices becomes a very vital issue. The Input devices like keyboards, mouse are used to feed data to the computer therefore the surveillance of input devices is much more important than monitoring the activity of users. A keylogger is a type of attack used by attackers that can capture keystrokes and save it to their database and send that data to the attacker, thus compromising the confidentiality of the victim. It is very dangerous to those systems that are used for daily transactional purposesie. Online banking.

Keywords—Keyloggers, security

Introduction:

Along with spyware, keylogging malware was ranked as the highest threat by the 2019 Global Threat Intelligence Report. In May 2019, version 9 of the Hawk Eye malware surfaced, targeting business users. The term "keylogger" refers to a type of malware that captures the input of a user's keyboard in order to retrieve information about them. Keyloggers, in common with many trojans, are designed to mimic legitimate software and bypass anti-virus or anti-malware scanners [6]. It is observed that around 90%
of keyloggers exist in userspace which makes them almost impossible to detect and remove [7]. There are two types of keyloggers, hardware keyloggers and software keyloggers. As soon as the computer is turned on, the hardware keylogger is activated. Hardware keyloggers are of various types like, keyboard overlays, keyboard commands, etc. In software keylogger, the software code gets executed only when the software is executed.

Literature Survey:

In the first paper [1] to detect and prevent keylogger spyware, the honey pot system is being used. When a particular process enters the system, it is simultaneously logged in the honeypot server, this server logs the mail sent by the process. If a mail is being sent to a particular mail id for a sustained amount of time, it raises an alert to the host system which then launches the signal to terminate the system.

In paper [2] mining techniques have been used to detect the spyware. Here, five different supervised learning algorithms were used to categorize the known spyware pattern called n-grams. This pattern of spyware includes keylogger and info-stealer patterns. The n-grams are drawn out from known software and spyware.

In paper [3], the author makes clear various anti-security design patterns that can be used as a measure for the detection of spyware. Here the author uses classifiers which detect the spyware from predefined types, already known to the system. Any new spyware then gets placed in a new family.

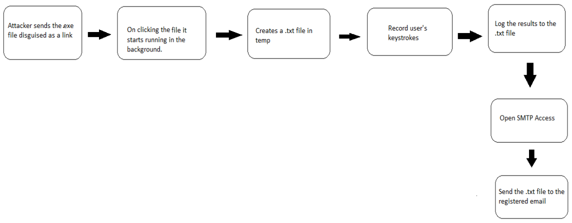
In paper [4] various techniques for detecting keyloggers are discussed. In Anti-hook mechanism, the system is scanned and each process is enumerated and checked for hook API usage. The safe access to password protected accounts technique, it is suggested that the user gives a sequence of strings between consecutive keys of password. The paper also discussed techniques such as bot detection, honey id and dendritic cell algorithm.

Paper [5] explains the keylogger designnpattern, its usage, how its implemented and embedded into an application. It also highlights the visible design patterns, which can be used to detect and differentiate between the types of keyloggers. From observations, it is concluded that the keylogger will create a file of all user actions. This file could then be shared to the malicious user.

Methodology:

In this demonstration, we have created a keylogger using python and converted it into an executable file using Auto PY to Exe. After clicking on this .exe file it starts running in the background and creates a .txt file in temp. It is now ready to listen to keystrokes. All the keystrokes are recorded, and the result is logged to the .txt file. It now sends the .txt file to the registered email using the SMTP protocol. The time for which this file runs can be configured in the code. Libraries used:

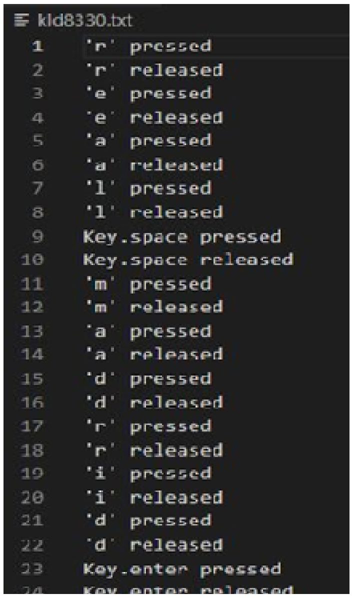
- email
- smtplib
- pynput
- Time
- threading


Attacker sends the.exe file disguised as a link
On clicking the file it starts running in the background.
Creates a .txt file in temp
Record user's keystrokes
Log the results to the .txt file
Open SMTP Access
Send the .txt file to the registered email

Block diagram fig. 1

Results and Discussion:

Here, it can be clearly seen that the target computer's keystrokes are recorded in text format and hence can be used against the victim and hence compromise his confidentiality, and personal and bank details can also be captured easily.


kld8330.txt

```
'r' pressed
'r' released
'e' pressed
'e' released
'a' pressed
'a' released
'l' pressed
'l' released
Key.space pressed
Key.space released
'm' pressed
'm' released
'a' pressed
'a' released
'd' pressed
'd' released
'r' pressed
'r' released
'i' pressed
'i' released
'd' pressed
'd' released
Key.enter pressed
Key.enter released
```

Conclusion:

Malwares are becoming a major threat to the world. We could divide keyloggers based n sentiments as positive and negative, positive use of keyloggers include parental monitoring, improve employee productivity, investigate writing, ethical hacking, forensic investigations, etc and negative uses include gathering information, recording screen and identity theft. Keyloggers mostly possess a menace touser privacy. The present was focused and simple keylogger and how it catches keystrokes from the target computer. The user could overcome this threat by using the KeyScambler program, install AntiLogger software, use a unique method when typing passwords, and fool the Keylogger with random typing.

Acknowledgement:

We sincerely thank Atharva College of Engineering and madam Supriya Dicholkar for the cooperation and support throughout the project at every step and guiding us throughout.

References:

[1] Mohammad Wazid, Avita Katal, R.H. Goudar,D.P. Singh and Asit Tyagi, "A framework for detection and prevention of novel keylogger spyware attacks", 2013 7th International Conference on Intelligent Systems and Control (ISCO).

[2] Raja khurranshahzad, Syed Imran Hyder, NiklasLavesson, "Detection of spyware by mining executable files", 2010 International Conference on Availability, Reliability and Security.

[3] Mohamed Adel Sheta , Mohamed Zaki , Kamel Abd El Salam El Hadad , H. Aboelseoud M, "Antispyware Security Design Patterns", 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC).

[4] A. Solairaj , S. C. Prabanand , J. Mathalairaj , C. Prathap , L. S. Vignesh, "Keyloggers software detection techniques", 2016 10th International Conference on Intelligent Systems and Control (ISCO).

[5] Christopher A. Wood, Rajendra K. Raj "Keyloggers in Cybersecurity Education", In Proceeding of the 2010 International Conference on Security and Management, pp. 293-299, July 12- 15,2010.

[6] Javaheri, D; Hosseinzadeh, M; Rahmani, M. 'Detection and elimination of spyware and ransomware by intercepting kernellevel system routines'. IEEE Access, Figure 7: of the art and challenges', 14th IEEE International Conference on Advanced Communication Technology (ICACT), Algorithm for the proposed virtual keyboard. Figure 8: Comparing the proposed virtual keyboard with QWERTY and ABC keyboards. February 2020 Network Security 19 FEATURE www.networksecuritynewsletter.com A SUBSCRIPTION INCLUDES: Online access for 5 users An archive of back issues Volume 6, 2018. DOI: 10.1109/ ACCESS.2018.2884964.

[7] P. Phule, "Unintentional Use of USB Channels and Protection," International Journal of Current Engineering and Technology, vol. 5, 2015.

[8] Danial Javaheri ,Mehdi Hos seinzadeh , Amir Masoud Rahmani , "Detection and Elimination of Spyware and , Ransomware by Intercepting KernelLevel System Routines", 2018 Page s: 78321 – 78332,IEEE Access.

[9] M. S. Hasibuan, "Keylogger Pada AspekKeamananKomputer [Keylogger on Computer Security aspect]," JurnalTeknovasi, vol. 03, pp. 8-15.

[10] Ming-Wei Wu, Yi-Min Wang, Yennun Huang, "Self HealingSpyware : Detection and Remediation ",2007,Pages:588-596,IEEE Transactions on Reliability, IEEE Journals