IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

Keystroke Logging for Activity-Monitoring using Python

Himanshu[1], Sachin Kaushik[2], Pankaj Kumar[3], Vimmi Malhotra[4]
Students, Department of Computer Science Engineering[1,2,3]
Assistant Professor, Department of Computer Science Engineering[4]
Dronacharya College of Engineering, Gurugram, India

Abstract: *Cyberwarfare is observed very frequently as always some or the other country is targeting to ruin its enemy country by hacking confidential data from vital computer systems. This has led to dangerous international conflicts. Hence, to avoid illicit entry of other than military person or a government official several tools are being used today as spyware. Keyloggers are one of the prominent tools which are used in today's world to obtain secret or confidential data of a legitimate and contradictory a malicious user too. These keyloggers are advantageous and taken up positively for monitoring employee productivity, for law enforcement and the search for evidence of the crime. While it's negative illegitimate use includes data theft and passwords. The keylogger is today witnessed as a malicious attack and is looked upon as a security threat. But every coin has two sides. Keylogger actually helps in avoiding several security breaches and also aids in detecting several crimes across the net world followed by other fellow countries. This fact has motivated to write this paper and as a consequence, an experimental analysis too was carried out in order to conclude that keyloggers' log file helps identify the person by analyzing proper pattern of the words entered in the file. This paper focuses majorly on the aspect of natural language processing, where a log file obtained thru keylogger software is thoroughly processed via the algorithm as described in the paper. The results yielded a fair understanding of the results obtained as one can easily identify the words used and on the basis of that can also know the type of person on the other end with his ideas, malicious one or of a legal kind*

Keywords: Keyloggers, Spyware, Cyberwarfare, Cyberwar

REFERENCES

[1]. R. K. R. Venkatesh, "User Activity Monitoring Using Keylogger.," Asia Journal of Information Technology, vol. 15, no. 23, pp. 47584762., 2015.
[2]. P. T. Sahu, " System Monitoring and Security Using Keylogger.," International Journal of Computer Science and Mobile Computing, vol. 2, no. 3, pp. 106-111, 2013.
[3]. D. R. John Deluca, "A System-Wide Keystroke Biometric System.," Proceedings of Student-Faculty Research Day, CSIS, Pace University , 2011.
[4]. L. Nystrom,
[5]. "https://vtnews.vt.edu/articles/2010/11/111110-engineering-yao.html., " https://vtnews.vt.edu/articles/2010/11/111110- engineeringyao.html, March 2011.
[6]. J. V. MdLiakat Ali, "Keystroke Biometric Systems for User Authentication.," Springer, 2016.
[7]. N. L. JoëlPlisson, "A Rule based Approach to Word Lemmatization.," Proceedings of IS-2004, researchgate.net, 2004.
[8]. M. R. Dr. S.Vijayaran, "Text mining: open source tokenization tools – an analysis.," Advanced Computational Intelligence: An International Journal (ACII), vol. 3, no. 1, 2016.
[9]. S. R. MayukhRath, "Semi Supervised NLP Based Classification of Malware Documents.," International Conference on Information Systems Security, Springer , 2017.