Abstract

Spyware is considered as a great threat to confidentiality that it can cause loss of control over private data for computer users. This kind of threat might select some data and send it to another third party without the consent of the user. Spyware detection techniques have been presented traditionally by three approaches; signature, behavior and specification based detection techniques. These approaches were successful in detecting known spyware but it suffers from some drawbacks such as; the need for updating data describing the system behavior to detect new or unknown spywares, and the high level of false positive or false negative rate. Therefore, in this paper we introduce a proposed anti spyware system design and implementation using design patterns for detecting and classifying spyware. This proposed approach can be reusable and modifying itself for any new or unknown spyware.
1. G. Padmavathi, and S. Divya “A Survey on Various Security Threats and Classification of
Malware Attacks, Vulnerabilities and Detection Techniques”, The International Journal of
Codes Similarity Using N-Gram and Vector Space Model”, IEEE International Conference on
information and applications (ICISA), pp. 1-4, Republic of Korea, 2011.
International Journal of Engineering Research & Technology (IJERT), Vol. 2, pp. 61-68, India,
2013.
Combination Technique and Signature Generation”, IEEE International Conference on
5. Raja Khurram Shazhad, Syed Imran Haider, and Niklas Lavesson “Detection of Spyware
by Mining Executable Files”, IEEE International Conference on Availability, Reliability and
6. Kai Huang, Yanfang Ye, and Qinshan Jiang “ISMCS: An Intelligent Instruction Sequence
based Malware Categorization System”, IEEE International Conference of Anti-counterfeiting,
7. Mohammad Wazid, Avita Katal, R.H. Goudar, D.P. Singh, and Asit Tyagi “A Framework
for Detection and Prevention of Novel Keylogger Spyware Attacks”, IEEE International
8. Karan Sapra, Benafsh Husain, Richard Brooks, and Melissa Smith “Circumventing
Keyloggers and Screen dumps”, IEEE International Conference on Malicious and Unwanted
9. Raihana Md Saidi, Siti Arpah Ahmad, Noorhayati Mohamed Noor, and Rozita Yunos
“Windows Registry Analysis for Forensic Investigation”, IEEE International Conference on
Technological Advances in Electrical, Electronics and Computer Engineering (TAECE), pp.
10. Raja Khurram Shahzad, Niklas Lavesson, and Henric Johnson “Accurate Adbware
Detection using Opcode Sequence Extraction”, IEEE International Conference on Availability,
11. Raja Khurram Shahzad and Niklas Lavesson “Detecting scareware by mining variable
length instruction sequences”, IEEE International Conference on Information Security South
12. E. Gamma, R. Helm, R. Johnson, and J. Vlissides, Design Patterns: Elements of
Reusable Object-Oriented Software, Boston, Massachusetts, Addison-Wesley Longman
13. Eric Freeman, Elisabeth Freeman, Bert Bates, and Kathy Sierra, Head First Design
Patterns, O’Reilly Publishing Co., Inc., USA, 2008.

Index Terms

Computer Science Security
Keywords

Spyware, Design patterns