Abstract

Human society is moving towards a life that is fully governed by automated systems where every important event of our life is locked and protected by a 'String', known as password. Password protection is in high demand and researchers have shown fervent interest to accomplish the same. Besides, the process of stealing information also evolving. Keystrokes monitoring by using keylogger is an advanced way to steal passwords and valuable data. As keylogger is an unprivileged program running on user-space, it could be injected through many different ways into a computer. Usually, keylogger is untraceable by the user and also undetectable by various known anti-viruses. Many cyber security specialists have proposed different methods for detection of this malicious program which includes API based detection method and network traffic monitoring system. But, with evolving technology, attackers have developed a new level of keylogger which is no longer easily detected though those conventional methods. This new level of keyloggers is capable of communicating with the eavesdropper without sending any attached file and uses volatile memory as a buffer. In this paper, we have proposed a memory
Keylogger Detection using Memory Forensic and Network Monitoring

analysis based detection method. This proposed method is capable of detecting such different type of logger and also works for on traditional one. With this method any regular user can detect any suspicious activity. And also it does not need any special permission from operating system. It was tested on Linux and Windows OS with satisfactory level of success.

References

4. “Unprivileged detection of user space keyloggers” by Mugdha Kolte from MITCOE International Journal of Innovation Research in Science, Engineering and Technology
7. R Sreeram Sreenivas, Dr R Anitha; Detecting keyloggers based on traffic analysis with periodic behavior; PSG College of Technology, Coimbatore, India

Index Terms

Computer Science Security
Keywords

Keylogger, volatility, user space, memory forensic, wireshark, SMTP, HTTP, key strokes.