Investigation of State Division in Botnet Detection Model

Wei WAN*,**, Jun LI*,**

* University of Chinese Academy of Sciences, Beijing, China

** Computer Network Information Center of Chinese Academy of Sciences, Beijing, China

wanwei@cstnet.cn, jlee@cstnet.cn

***Abstract*—Botnet as a new technology of attacks is a serious threat to Internet security. With the rapid development of the botnet, botnet based several protocols came into being. In accordance with the feature of botnet, the Hidden Markov Model has application in botnet detection. Firstly, according to the situation and problems of the botnet recently, the life cycle and behaviour characteristics of the botnet have been analysed. After that a mathematical model based on state division has been built to describe the botnet. Meanwhile, a method of botnet detection based on this model has been proposed. Finally, we analyzed and summarized the experimental results, and verified the reliability and rationality of the detection method.**

***Keyword*—Botnet, Hidden Markov Model, State Division**

Wei WAN received the B.S. degrees from Beijing Information Technology Institute in 2004, and M.S. degrees from Graduate University of Chinese Academy of Sciences. Now he is currently working toward Ph.D. degree at University of Chinese Academy of Sciences. He is working at Computer Network Information Center of Chinese Academy of Sciences. His research interests include network security.

Jun LI is Ph.D, research fellow-professor, Ph.D tutor, Vice Chief Engineer of Computer Network Information Center of Chinese Academy of Sciences. His research interests include network security, network architecture.