The prevention threat of behavior-based signature using pitcher flow architecture

Abstract

In recent years, Intrusion Prevention System (IPS) has been widely implemented to prevent suspicious threats. Unlike the traditional Intrusion Detection System, IPS has additional features to secure the computer network system. IPS is an access control device with a prevention function, which enforces a network security policy, is a helpful device that allows for more granular blocking action. In this paper, we propose a new prediction and prevention method with behavior-based detection, this method is called pitcher flow. We describes the habitual activity of the performance an overall network with a new algorithm for identifying and recognizing the normal behavior of user activities in the internal network. First, we define behavior activity by duration of activity conducted and active connection. Second, we categorize packets into class/type, identifying parameters by classifying the packets. Finally, we use the pitcher flow mechanism to identify and recognize suspicious threats. This paper also describes an algorithm for the complexity of the suspicious response.