عنوان مقاله:

Botnet Detection Based on Behavioral Patterns using Netflow Records

محل انتشار:

هشتمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1398)

تعداد صفحات اصل مقاله: 8

نویسنده:

Atieh Bakhshandeh - *Afta Department Research Center for Development of Advanced Technologies Tehran, Iran*

خلاصه مقاله:

Botnets are networks which are composed of compromised computers (called bots) with the aim of launching different kind of attacks such as DDoS, spamming and fishing. Most IDS/IPS systems use signature-based techniques to detect botnets in a network. However, botnets often can be identified by their footprints at network level, since they have specific behavioral patterns when they make connections to their command and control(C&C) servers. Furthermore, Detecting attacks at network level can be achieved using a shorter version of the traffic called Netflow which does not contain packet payloads providing more confidentiality and less storage overhead. In [S. García, HackLu 2014 at Luxemburg] a behavioral model was represented that accurately models botnet actions. In this paper, we utilize their behavioral features to train a more efficient and accurate model which does not have the intrinsic shortcomings of their suggested model. We also make their dataset balanced using a standard method which leads to even better results. The results have shown significant improvements over the previous method both in accuracy and .efficiency. It is indicated that this method can be effectively used in production environments for detecting botnets

کلمات کلیدی:

;Botnet; C&C channels; Netflow; Behavioral pattern

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1010091