

عنوان مقاله:

HF-Blocker: Detection of Distributed Denial of Service Attacks Based On Botnets

محل انتشار:

مجله پیشرفت در مهندسی کامپیوتر و فناوری، دوره 1، شماره 3 (سال: 1394)

تعداد صفحات اصل مقاله: 7

نویسندگان:

Bitra Amirshahi - *Department of Computer Engineering and Information Technology, Payame Noor University, PO BOX 19395-3697 Tehran, IRAN*

Ali Ahangari - *Department of Computer Engineering and Information Technology, Payame Noor University, PO BOX 19395-3697 Tehran, IRAN*

خلاصه مقاله:

Abstract—Today, botnets have become a serious threat to enterprise networks. By creation of network of bots, they launch several attacks, distributed denial of service attacks (DDoS) on networks is a sample of such attacks. Such attacks with the occupation of system resources, have proven to be an effective method of denying network services. Botnets that launch HTTP packet flood attacks against Web servers are one of the newest and most troublesome threats in networks. In this paper, we present a system called HF-Blocker that detects and prevents the HTTP flood attacks. The proposed system, by checking at the HTTP request in three stages, a Java-based test, check cookies and then check the user agent, detects legitimate source of communication from malicious source, such as botnets. If it is proved the source of connection to be bot, HF-Blocker blocks the request and denies it to access to resources of the web server and thereby prevent a denial of service attack. Performance analysis showed that HF-Blocker, detects and prevents the HTTP-based attacks of botnets with high probability.

کلمات کلیدی:

botnet, web servers, DDoS attacks, HTTP, HTTP Flood

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/892698>

