World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:06, 2018

Web Proxy Detection via Bipartite Graphs and One-Mode Projections

Authors : Zhipeng Chen, Peng Zhang, Qingyun Liu, Li Guo

Abstract : With the Internet becoming the dominant channel for business and life, many IPs are increasingly masked using web proxies for illegal purposes such as propagating malware, impersonate phishing pages to steal sensitive data or redirect victims to other malicious targets. Moreover, as Internet traffic continues to grow in size and complexity, it has become an increasingly challenging task to detect the proxy service due to their dynamic update and high anonymity. In this paper, we present an approach based on behavioral graph analysis to study the behavior similarity of web proxy users. Specifically, we use bipartite graphs to model host communications from network traffic and build one-mode projections of bipartite graphs for discovering social-behavior similarity of web proxy users. Based on the similarity matrices of end-users from the derived one-mode projection graphs, we apply a simple yet effective spectral clustering algorithm to discover the inherent web proxy users behavior clusters. The web proxy URL may vary from time to time. Still, the inherent interest would not. So, based on the intuition, by dint of our private tools implemented by WebDriver, we examine whether the top URLs visited by the web proxy users are web proxies. Our experiment results based on real datasets show that the behavior clusters not only reduce the number of URLs analysis but also provide an effective way to detect the web proxies, especially for the unknown web proxies.

Keywords : bipartite graph, one-mode projection, clustering, web proxy detection
Conference Title : ICICS 2018 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 06-07, 2018