World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:8, No:12, 2014

Study on Network-Based Technology for Detecting Potentially Malicious Websites

Authors : Byung-Ik Kim, Hong-Koo Kang, Tae-Jin Lee, Hae-Ryong Park

Abstract : Cyber terrors against specific enterprises or countries have been increasing recently. Such attacks against specific targets are called advanced persistent threat (APT), and they are giving rise to serious social problems. The malicious behaviors of APT attacks mostly affect websites and penetrate enterprise networks to perform malevolent acts. Although many enterprises invest heavily in security to defend against such APT threats, they recognize the APT attacks only after the latter are already in action. This paper discusses the characteristics of APT attacks at each step as well as the strengths and weaknesses of existing malicious code detection technologies to check their suitability for detecting APT attacks. It then proposes a network-based malicious behavior detection algorithm to protect the enterprise or national networks.

Keywords : Advanced Persistent Threat (APT), malware, network security, network packet, exploit kits
Conference Title : ICCNSS 2014 : International Conference on Computer Networks and Systems Security
Conference Location : Melbourne, Australia
Conference Dates : December 16-17, 2014