Abstract

The botnet is controlled by an attacker, which is formed by a lot of vulnerable hosts. The botnet is one of the biggest threats on the Internet. The attacker usually uses it to attack, such as: spam, distributed denial of service attacks, fraud and so on. In this paper, we mainly study the control channel of the botnet, including the IRC protocol, the P2P protocol and the HTTP protocol. At the same time, this paper also studies the detection method of the botnet, which includes the host based detection method and the network based detection method.

References


11. C. Kalt, Internet Relay Chat: Client protocol, Request for Comment (RFC) 2812 (Informational), 2000


14. Jun Li, Toby Ehrenkranz, Geoff Kuenning, Simulation and Analysis on the Resiliency and Efficiency of malnets. Workshop on Principles of Advanced and Distributed Simulation (PADS’05), 2005


21. P. Szor, The Art of Computer Virus Research and Defenses, Addison-Wesley Professional, 2005


Index Terms

Computer Science  Security

Keywords

Botnet, Command and Control, P2P, Detection, DDoS.