Among the diverse forms of malware, Botnet is the serious threat which occurs commonly in today’s cyber attacks and cyber crimes. Botnet are designed to perform predefined functions in
an automated fashion, where these malicious activities ranges from online searching of data, accessing lists, moving files sharing channel information to DDoS attacks against critical targets, phishing, click fraud etc. Existence of command and control (C&C) infrastructure makes the functioning of Botnet unique; in turn throws challenges in the mitigation of Botnet attacks. Hence Botnet detection has been an interesting research topic related to cyber-threat and cyber-crime prevention. Various types of techniques and approaches have been proposed for detection, mitigation and prevention to Botnet attack. This paper, discusses in detail about Botnet and related research including Botnet evolution, life-cycle, command and control models, communication protocols, Botnet detection, and Botnet mitigation mechanism etc. Also an overview of research on Botnets which describe the possible attacks performed by various types of Botnet communication technologies in future.

Reference

- A. Schonewille and D. van Helmond, “The domain name service as an IDS”, Research Project for the Master System-and Network Engineering at the University of Amsterdam, 2006.
- H. Binsalleeh, T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, and L.
- Rajab, M., Zarfoss, J., Monroe, F., & Terzis, A. (October 2006). “A multifaceted approach to understanding the botnet phenomenon” Retrieved October 31, 2009 from
http://www.imconf.net/imc-2006/papers/p4-rajab.pdf
- Prosenjit Sinha, Amine Boukhtouta, Victor Heber Belarde, Mourad Debbabi, "Insights from the Analysis of the Mariposa Botnet"
- SANS Institute InfoSec Reading Room provided a description on "Bot & Botnet: An overview" research on topics in information security, 2003.
- Xuhua Ding, Wei Yu, Ying Pan, "A Dynamic Trust Management Scheme to Mitigate Malware Proliferation in P2P Networks" IEEE conference on communications, 2008.
- Communications protocol at http://en.wikipedia.org/wiki/Communications_protocol

Index Terms

Computer Science

Communications
Key words

Bot  Communication protocols  Honeynet

Attacks

Preventaation

Mitigation

C&C mechanism

Botnet