Abstract

Botnet has recently been recognized as one of the most significant security threats/worms of the Internet. Latest attacks are increasingly complex, and utilize many strategies in order to perform their intended malicious/hazardous task. Attackers have developed the ability of controlling vast area of infected hosts, characterized by complex executable command set, each involved part in cooperative and coordinated attacks. These papers propose the advanced approach related botnet detection and analysis in the near future. It demonstrates a novel approach of botnet investigations and defense mechanisms.


P. Kalakota and C. T. Huang, "On the benefits of early filtering of botnet unwanted traffic," in Proceedings of 18th International Conference on Computer
- D. Dagon, C. Zou, and W. Lee, &quot;Modeling botnet propagation using time zones,&quot; in Proceedings of the 13th annual network and distributed system security symposium (NDSSâ€™06), 2006.
- J. C. Wierman and D. J. Marchette, &quot;Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction,&quot; Computational Statistics & Data Analysis, vol. 45, pp. 3-23, 2004.

Index Terms

Computer Science
Security
Keywords
  Bots  Botnet  C&C  Analysis