

An efficient soft computing approach for securing information over GAMEOVER Zeus Botnets with modified CPA algorithm

Authors: **S. Aanjankumar** S. Poonkuntran

Soft Computing - A Fusion of Foundations, Methodologies and Applications Volume 24 Issue 21 Nov 2020 pp 16499–16507 <https://doi.org/10.1007/s00500-020-04956-y>

Abstract

In recent times, security threats are predominant in almost all digital applications over the internet. One such threatening effect comes from GAMEOVER Zeus Botnet. These Botnets enter inside online networks and affect the Peer client list, through Internet Relay Chat (IRC). IRC includes applications like Tactical chat and On Chat. Zeus botnets gather the secret information of these users, such as bank data and military secrets. Moreover, the architecture is P2P and hence the location of GAMEOVER Zeus Botnet varies from the one to another botnets models. The threat of Zeus botnets loom large as they operate through the processes of identification of users, through which, they establish control over the hosts via P2P server. An intelligent method of identification of Zeus botnets in a distributed computing system using cryptographic schemes to defend against such attacks is the prime issue of research in this paper. An advanced Botnet capturing algorithm, named as modified cryptographic prefix IP anonymised (CPA) algorithm is proposed in this research paper to effectively counter the threats of Zeus bots. Essential features of the proposed CPA algorithm include prefixed IP mapped anonymising in Internet Relay Chat, inbuilt adaptive security algorithm, which helps in network cleansing. If left unchecked, these Zeus botnets may result in consequent shutdown of the system. Hence, identification of the location of these botnets with the help of IP-prefix mapped method through modified CPA algorithm have been systematically presented in this paper.