



RESEARCH ARTICLE

An Efficient Methodology for Detecting Spam Using Spot System

MRS. SARANYA.S¹, MRS. R.BHARATHI²

¹M.TECH (Computer Science & Engineering), PRIST UNIVERSITY, Pondicherry

²Assistant Professor (Computer Science & Engineering), PRIST UNIVERSITY, Pondicherry

Email: ¹saranya.sekar@yahoo.com, ²prist2009cse@gmail.com

Abstract—Major Security challenge on the Internet is the existence of the large number of compromised machines. Compromised machines on the Internet are generally referred to as bots, and the set of bots controlled by a single entity is called a botnet. Botnets have multiple nefarious uses: mounting Distributed denial of service attacks, stealing user passwords and identities, generating click fraud, and sending spam email. Compromised machines are one of the key security threats on the Internet. Given that spamming provides a key economic motivation for attackers to recruiting the large number of compromised machines, and focus on the detection of the compromised machines in a network that are involved in the spamming activities, commonly known as spam zombies. Develop an effective spam zombie detection system named SPOT by monitoring outgoing messages of a network. SPOT is designed based on a powerful statistical tool called Sequential Probability Ratio Test, which has bounded false positive and false negative error rates. The number and the percentage of spam messages originate by spam detection technique.

Keywords—Compromised machines; spam zombies; spam detection techniques; spot detection system.

Full Text: <http://www.ijcsmc.com/docs/papers/January2014/V3I1201418.pdf>