Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.568 – 573

RESEARCH ARTICLE

A Novel Approach of Detecting the Camouflaging Worm

HEMALATHA R[1], S. PRATHIBA[2]
[1]Department of Information Technology, Bharath University, India
[2]Department of Information Technology, Bharath University, India

Abstract— Active worms major security threats to the Internet. This is due to the ability of active worms to propagate in an automated fashion as they continuously compromise computers on the Internet. Active worms evolve during their propagation, and thus, pose great challenges to defend against them. In this paper, we investigate a new class of active worms, referred to as Camouflaging Worm (C-Worm in short). The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm detection systems based on analysing the propagation traffic generated by worms. We analyse characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and nonworm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, the design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, we show the generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.
In the existing system, traditional worms are more threats to the internet and also would produce lot of overall network traffic. It is very easy to identify the worm using traditional worm detection as the overall network traffic is increased. In the proposed model, camouflage worm is modelled and detection using spectrum based approach. Worm targets only vulnerable node so that overall traffic level is not increased. Spectrum based approach which is used to kill the C-worm. Modifications are mode in designing a worm which is used to increase the CPU load in the system, and also compared with traffic level of an application initiation and the C-worm. This process makes very clear process of execution.

Key Terms: - Worm; Camouflaging Worm; Power Spectral Density; Spectral Flatness Measure

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I42013123.pdf