Chapter 27
Early Worm Detection for Minimizing Damage in E-Service Networks

Tarek S. Sobh
Egyptian Armed Forces, Egypt

Heba Z. El-Fiqi
Zagazig University, Egypt

ABSTRACT

One of the most powerful weapons for attackers is the Internet worm. Specifically, a worm attacks vulnerable computer systems and employs self-propagating methods to flood the Internet rapidly. Since a "Worm" is self-propagated through the connected network, it doesn't need human interaction or file transmission to replicate itself. It spreads in minutes; Slammer worms infect about 75,000 nodes through the internet in about 10 minutes. Since most of antivirus programs detect viruses based on their signature, then this approach can't detect new viruses or worms till being updated with their signature, which can't be known unless some systems had already been infected. This highlights worms are still on the top of malware threats attacking computer systems, although the evolution of worms detection techniques. Early detection of unknown worms is still a problem. This chapter produce a method for detecting unknown worms based on local victim information. The proposed system uses Artificial Neural Network (ANN) for classifying worm/ nonworm traffic and predicting the percentage of infection in the infected network. This prediction can be used to support decision making processes for network administrators to respond quickly to worm propagation in an accurate procedure.

INTRODUCTION

Network attacks such as computer virus and worms that scan computers randomly have caused billions of dollars in damage to enterprises across the Internet [Erbschloe M., 2005]. There are different worm detection techniques. [Guofei, G., 2004] classified them according to the worm characteristic used by detection technique. One approach is using worm signatures, it depends on the identical or similar traffic the worm causes while spreading, but it is only effective if worm signatures are known, so it cannot detect zero-day and polymorphic worms. By using polymorphic

DOI: 10.4018/978-1-61520-789-3.ch027

payloads, instead of static signature, the worm can evade detection [Nazario J., 2004].

There is another approach which depends on the Internet Control Message Protocol (ICMP) packet analysis. Due to random scanning behavior of worms, these scans often reach inactive IP addresses. But this approach focuses on global strategies and requires a large monitored network.

The computer worm, which is a self-propagating malicious code, spread themselves without any human interaction and launches the most destructive attacks against computer networks. Since worm exploits a security vulnerability corresponding to a specific network port number, Vulnerable hosts exhibit infection-like behavior when infected. Researchers use this observation as base for worm detection approaches. Nazario [Nazario J., 2004] produces destination port as one of the basic parameters that is used to describe the signature of the worm. For worms that target Web servers, this would be set to port 80. Other worms that attack other applications would use different ports. [Chen X. & Heidemann J., 2004], [Guofei, G., 2004], and Michael [Michael, L., 2003] uses this idea to build their worm detection models. Previous work uses anomaly method [Guofei, G., 2004] or mathematical model [Chen X. & Heidemann J.,2004] to produce the maximum number of packets received by a port that produces non-worm traffic. Most of previous work could not predict the new value if the behavior of this network is changed and could not detected slow worm.

[Li, P., M. Salour, & X. Su, 2008] describes the worm's life as consisting of many phases: target finding, transferring, activation, and infection. The first two phases cause network activities, worm behaviours in these two phases are critical for developing detection algorithms. A Supervised Artificial Neural Network (ANN) can be trained to take the values that represent the current behavior of the network under non-worm traffic and worm traffic. After sufficient number of iterations, it can be used as a control unit in the proposed system to identify the worm traffic. Then packet filter can be used to stop the worm's spread by filtering Transmission Control Protocol (TCP) port at the border of the network. This chapter produces an artificial intelligence system for worm detection, that can detect worm virus in network with accuracy of %99.96.Also this system can predict the percentage of worm infection in the network with absolute error average from 0% to 4%.

BACKGROUND

Since the Morris worm arose in 1988, Internet worms have been a persistent security threat, for example, the Code Red worm compromised at least 359,000 machines in 24 hours on July 19, 2001 [Chen Z., 2007]. The Slammer worm was unleashed with a 376-byte user datagram protocol (UDP) packet and infected more than 90% of vulnerable hosts in 10 minutes on January 25, 2003 [Chen Z., 2007]. These active worms caused large parts of the Internet to be temporarily inaccessible and cost both public and private sectors millions of dollars. Moreover, the frequency and the virulence of active-worm outbreaks have been increasing dramatically in the last few years, presenting a significant threat to today's Internet. Therefore, it is imperative to characterize the worm attack behaviors, analyze Internet vulnerabilities, and study countermeasures accordingly.

Malware in Network Attacks

Malicious code is a software or firmware that is intentionally placed in a system for an unauthorized purpose. Some of its basic types are *Trojans*, *Viruses*, and *Worms*.

Trojan horses are both problematic and a basic type of malicious code designed primarily to give attackers access to system files [Erbschloe M., 2005]. Trojan horse may be written to steal logon passwords, log user keystrokes, or even allow an attacker full administrative control on the targeted computer. This type of malicious code is contained