Abstract

The effort required for detecting worm that threaten the reliability and stability of network resources is in the process of advancing, demanding increasingly sophisticated resources. A worm is a self-propagating program that infects other hosts based on a known vulnerability in network hosts. The spread of active worms does not need any human interaction. There is a growing demand for effective techniques to detect the presence of worms and to reduce the worms spread. Worms have become a major threat to the Internet due to their ability to rapidly, compromise large numbers of computers. This work presents a comparative analysis of behavioural classification of networks (BCN) and early warning system (EWS) to determine which one performs better in computer worm detection.

References

- Shigang Chen, Sanjay Ranka 2004 Detecting Internet Worms at Early Stage

Index Terms

Computer Science

Security

Keywords

Nowadays excellent technology (i.e. anti-worms software packages) exists for detecting and eliminating known malicious codes. Typically anti-worms software packages inspect each file that enters the system looking for known signs (signatures) which uniquely identify an instance of known malicious codes. Nevertheless anti-worms technology is based on prior explicit knowledge of worm code signatures and cannot be used for detecting unknown worm codes. Following the appearance of a new worm a patch is provided by the operating system provider (if needed) and the anti-worm vendors update their signature-base accordingly. This solution is not perfect since worms propagate very rapidly and by the time local anti-worm software tools have been updated very expensive damage would have been inflicted by the worm.