Abstract

Computer worm detection has been a challenging and often elusive task. This is partly because of the difficulty of accurately modeling either the normal behavior of computer networks or the malicious actions of computer worms. This paper presents a literature review on the worm detection techniques, highlighting the worm characteristics leveraged for detection and the limitations of the various detection techniques. The paper broadly categorizes the worm detection approaches into content signature based detection, polymorphic worm detection, anomaly based detection, and behavioral signature based detection. The gap in the literature in the techniques is indicated and is the main contribution of the paper.

References

victims of an internet worm. In the proceedings of the internet Measurement Workshop
- Staniford, S. , Paxson, V. , & Weaver, N. 2002. How to Own the Internet in Your Spare
  Time. In USENIX Security Symposium, 149-167
  Communications Surveys & Tutorials, IEEE, 10(1), 20-35
- Weaver, N. , Paxson, V. , Staniford, S. , & Cunningham, R. 2003. A taxonomy of
  Fingerprinting. In OSDI Vol. 4.
  SIGCOMM workshop on mining network data, 165-170.
  Signature Detection. In USENIX security symposium, Vol. 286
- Kruegel, C. , Kirda, E. , Mutz, D. , Robertson, W. , & Vigna, G. 2006. Polymorphic worm
  detection using structural information of executables. In Recent Advances in Intrusion
  Detection, 207-226. Springer Berlin Heidelberg
  polymorphic internet worms. Parallel and Distributed Systems, IEEE Transactions on,
  18(7), 879-892
- Wang, L. , Li, Z. , Chen, Y. , Fu, Z. , & Li, X. 2010. Thwarting zero-day polymorphic
  worms with network-level length-based signature generation. IEEE/ACM Transactions on
  Networking (TON), 18(1), 53-66.
- Kinder, J. , Katzenbeisser, S. , Schallhart, C. , & Veith, H. 2010. Proactive detection of
  computer worms using model checking. Dependable and Secure Computing, IEEE
  Transactions on, 7(4), 424-438.
  detection and profiling. Knowledge and information systems, 18(2), 231-262
  towards an established taxonomy. Journal in computer Virology, 4(3), 251-266
- Li, J. , Stafford, S. , & Ehrenkranz, T. 2006. SWORD: Self-propagating worm
- Mahoney, M. V. , & Chan, P. K. 2001. PHAD: Packet header anomaly detection for
  identifying hostile network traffic.
- Gu, G. , Sharif, M. , Qin, X. , Dagon, D. , Lee, W. , & Riley, G. 2004. Worm detection,
  early warning and response based on local victim information. In Computer Security


**Index Terms**

Computer Science  
Security

**Keywords**

Computer worm  
computer worm detection  
intrusion detection  
detection techniques