Abstract

The paper presents the design of an integrated malware collection and analysis framework for botnet tracking. In proposed framework we have used Honypots as malware capturing tool. The proposed system design is unique in the sense that the information regarding the configuration of honeypot on which malware sample has been captured is saved with malware sample in the malware data-base. This system configuration information saved with the malware sample is used at the time of dynamic malware analysis for creating malware execution environment. As an execution environment thus created is analogous to environment in which malware was
captured therefore it generates true expected execution behavior leading to capturing of accurate execution traces. Further we have demonstrated the effectiveness of the proposed solution with the help of a prototype system.

References

- John Levine, Richard LaBella, Henry Owen, Didier Contis, Brian Culver “The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks” School of Electrical and Computer Engineering
- Vinod Yegneswara, Paul Barford, Vern Paxson “Using Honeynets for Internet Situational Awareness”
  - http://securityresponse.symantec.com/avcenter/
  - http://www.caida.org/analysis/security/witty/
- Cliff Chang Chun Zou, Lixin Gao, Weibo Gong, Don Towsley “Monitoring and Early Warning for Internet Worms” University of Massachusetts at Amherst
- David Moore, Vern Paxson, Colleen Shannon, Stuart Staniford, Nicholas Weaver “The Spread of the Sapphire/Slammer Worm”, 2003
- Leurre.com: on the Advantages of Deploying a Large Scale Distributed Honeynet Platform
  - www.viruslist.com/de/viruses/encyclopedia?chapter=152540403
- Christopher Hecker, Kara L, Nance, and Brian Hay” Dynamic Honeypot Construction “
- Davide Cavalca and Emanuele Goldoni HIV E: an Open Infrastructure for Malware Collection and Analysis
  - J. Zhuge, T. Holz, X. Han, C. Song, and W.
An Integrated Framework for Malware Collection and Analysis for Botnet Tracking

Unpublished doctoral dissertation, Department of Information and Computer
- Saurabh Chamotra, Mr. Rakesh Kumar Sehgal, Dr. Raj Kamal “Honeysand: An Open Source Tools Based Sandbox Environment for Bot Analysis and Botnet tracking”
- Hengli Zhao, Ning Zheng, Jian Li, Jingjing Yao, Qiang Hou “Unknown Malware Detection Based on the Full Virtualization and SVM” 2009 International Conference on Management of e-Commerce and e-Government
- Trend Micro. Taxonomy of botnet threats (white paper), November 2006
- Saurabh Chamotra, Rakesh Kumar Sehgal Dr. Raj Kamal “J.S.Bhatia” Data Diversity of a Distributed Honeynet based malware collection system”, Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference
- Details of NOHA project: http://www.fp6-noah.org/publications/presentations/moeller-tfcsirt17.pdf
- Honeynet Project http://www.honeynet.org/
- L. Spitzner, Honeypots- Tracking Hackers, Indianapolis, IN: Addison-Wesley, 2003, pp. 242-261

Index Terms

Computer Science

Keywords
Culture
Productivity
Social Networks
Workplace
Malware
Hack