{tag} {/tag}

IJCA Special Issue on Communication Security

comnetcs - Number 1

Year of Publication: 2012

Authors:
Rakesh Kumar Sehgal

D. S. Bhilare

Saurabh Chamotra

{bibtex}comnetcs1010.bib{/bibtex}

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 Com puter 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 Changchun 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
- A. W. Jackson, D. Lapsley, C. Jones, M. Zatko, C. Golubitsky, and W. T.Strayer, “SLINGbot: A system for live investigation of next generation botnets,” in Cybersecurity Application and Technologies Conference for Homeland Security (CATCH), Washington, DC, USA, Mar. 2009.
- J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by irc nickname evaluation. In USENIX Workshop on Hot Topics in Understanding Botnets (HotBots’07), 2007.
- Reto Baumann and Christian Plattner, “White Paper: Honeynets”, 26 February 2002
- J. Yang, P. Ning, X. S. Wang, and S. Jajodia. Cards: A distributed system for detecting coordinated attacks. In SEC, 2000
- Iyad Kuwatly, Malek Sraj, Zaid Al Masri, and Hassan Artail. “A Dynamic Honeypot Design for Intrusion Detection” American U. of Beirut
- Christopher Hecker, Kara L, Nance, and Brian Hay” Dynamic Honeypot Construction “
- X. Jiang and D. Xu. Profiling self-propagating worms via behavioral footprinting. In Proceedings of CCS WORM , 2006
- F. Freiling, T. Holz, and G. Wicherski. Botnet tracking: Exploring a root-cause methodology to prevent denial-ofservice attaks. In ESORICS’05.g”
- Davide Cavalca and Emanuele Goldoni HIVE:an Open Infrastructure for Malware Collection and Analysis
- J. Zhuge, T. Holz, X. Han, C. Song, and W.
- Zou. Collecting autonomous spreading malware using high-interaction honeypots. In ICICS 2007, pages 438–451, 2007.
- M. Garetto, W. Gong, D. Towsley, “ModelingMalware Spreading Dynamics,” in Proc. of INFOCOM 2003, San Francisco, April, 2003.
- Liu, P. W. and Tyan, H. R, “An Adaptive defence mechanism for P2P Botnet.”

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
- P. Barford and V. Yegneswaran. An inside look at botnets.In Proc. Special Workshop on Malware Detection, Advancesin Information Security, 2006
- 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
- D. Moore. Network telescopes: Observing small or distant security events. In 11th USENIX Security Symposium, Invited talk, San Francisco, CA, Aug. 5–9 2002. Unpublished
- L. Spitzner. “Honeypot Farms”, Infocus, Aug. 2003. http://www.securityfocus.com/infocus/1720.
- DShield. Distributed Intrusion Detection System, www.dshield.org, 2007
- C. Leita , V.H. Pham , O. Thonnard , E. Ramirez-Silva ,F. Pouget , E. Kirda , M. Dacier , The Leurre.com Project: Collecting Internet Threats Information using a Worldwide Distributed Honeynet 2008 IEEE DOI 10.1109/WISTDE.2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing
- Mwcollect http://alliance.mwcollect.org.
- 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