Abstract

Botnets are considered one of the most dangerous and serious security threats facing the networks and the Internet. Comparing with the other security threats, botnet members have the ability to be directed and controlled via C&C messages from the botmaster over common protocols such as IRC and HTTP, or even over covert and unknown applications. As for IRC botnets, general security instances like firewalls and IDSes do not provide by themselves a viable solution to prevent them completely. These devices could not differentiate well between the legitimate and malicious traffic of the IRC protocol. So, this paper is proposing an IDS-based and multi-phase IRC botnet and botnet behavior detection model based on C&C responses messages and malicious behaviors of the IRC bots inside the network environment. The proposed model has been evaluated on five network traffic traces from two different network environments (Virtual network and DARPA 2000 Windows NT Attack Data Set). The results show that the proposed model could detect all the infected IRC botnet member(s), state their current status of attack, filter their malicious IRC messages, pass the other normal IRC messages and detect the botnet behavior regardless of the botnet communication protocol with very low false positive rate. The proposed model has been compared with some of the existing and well-known approaches, including BotHunter, BotSniffer and Rishi regarding botnet characteristics taken in each approach. The comparison showed that the proposed model has
made a progress on the comparative models by not to rely on a certain time window or specific bot signatures.

References

- Zhuge, J., Holz, T., Han, X., Guo, J. and Zou, W. 2007. Characterizing the IRC-based botnet phenomenon, Technical report, Peking University, University of Mannheim.
- Westervelt, R. 2011. Waledac Botnet showing resurgence with thousands of stolen email credentials. URL: http://searchsecurity.techtarget.com/news/1527003/Waledac-botnet-showing-resurgence-with-thousands-of-stolen-email-credentials.
- Neil, D., Stoppelman and Michael. 2007. The anatomy of clickbot. A, Proceedings of the ?rst conference on First Workshop, Hot Topics in Understanding Botnets, USENIX Association, Berkeley, CA, USA, pp. 11–11.
- Baecher, P., Koetter, M., T. Holz, M. D. and Freiling, F. 2006. The nepenthes platform: An ef?cient approach to collect malware, in K. C. Zamboni, Diego (ed.), Recent Advances in Intrusion Detection, Vol. 4219 of Lecture Notes in Computer Science, Springer Berlin, Heidelberg, pp. 165–184.
- Ioannidis, J. and Bellovin, S. M. 2002. Implementing pushback: Router-based defense against DDoS attacks, Proceedings of Network and Distributed System Security Symposium. Network and Distributed System Security Symposium: NDSS "apos;02 (Reston, Va.: Internet Society).
- Zeidanloo, H. R. and Manaf, A. B. A. 2010. Botnet detection by monitoring similar communication patterns, Journal of Computer Science 7(3): 36–45. URL: http://arxiv.org/abs/1004.1232.
- Gu, G., Junjie, Z. and Wenke, L. 2008. Botsniffer: Detecting botnet command and control channels in network traf?c, Technology 53(1): 1–13.
- Grizz Bard, J. B., Sharma, V., Nunnery, C., Kang, B. B. and Dagon, D. 2007. Peer-to-peer botnets: overview and case study, Proceedings of the ?rst conference on First Workshop on Hot Topics in Understanding Botnets, USENIX Association, Berkeley, CA, USA, pp. 1–1. URL: http://dl.acm.org/citation.cfm?id=1323128.1323129.
- Micro, T. 2006. Taxonomy of botnet threats, Malware White Papers pp. 1–15. URL: http://www.webbuyersguide.com/resource/resourceDetails.aspx?id=8021.
- Zeidanloo, H. R., Shooshtari, M., Amoli, P., Safari, M. and Zamani, M. 2010. A taxonomy of botnet detection techniques, Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference on, IEEE Computer Science and Information Technology, Chengdu, China, pp. 158 – 162.
- Honeynet Project 2006. Know your enemy: Honeynets, URL: http://www.honeynet.org/papers/honeynet.
- Baecher, P., Koetter, M., T. Holz, M. D. and Freiling, F. 2006. The nepenthes platform: An ef?cient approach to collect malware, in K. C. Zamboni, Diego (ed.), Recent Advances in Intrusion Detection, Vol. 4219 of Lecture Notes in Computer Science, Springer Berlin, Heidelberg, pp. 165–184.
- Zhichun, L., Anup, G. and Yan, C. 2008. Honeynet-based botnet scan traffic analysis, in W. C. D. D. Lee, Wenke (ed.), Botnet Detection, Vol. 36 of Advances in Information Security, Springer US, pp. 25–44.
- Goebel, J. and Holz, T. 2007. Rishi: identify bot contaminated hosts by IRC nickname evaluation, Proceedings of the First Workshop on Hot Topics in Understanding Botnets, USENIX Association, Berkeley, CA, USA, pp. 8–8. URL: http://dl.acm.org/citation.cfm?id=1323128.1323136.
- Liu, H., Sun, Y., Valgenti, V. C. and Kim, M. S. 2011. Trustguard: A flow-level reputation-based DDoS defense system, Consumer Communications and Networking Conference (CCNC), Washington State University, IEEE, Pullman, Washington 99164-2752, U.S.A.
- Binkley, J. R. and Singh, S. 2006. An algorithm for anomaly-based botnet detection, Vol. 06, USENIX Association, pp. 43–48.
- Stinson, E. and Mitchell, J. 2007. Characterizing bots remote control behavior, in B. M. Hammerli and S. Robin (eds), Detection of Intrusions and Malware, and Vulnerability Assessment, Vol. 4579 of Lecture Notes in Computer Science, Springer Berlin, Heidelberg, pp. 89–108.
- Gu, G., Yegneswaran, V., Porras, P., Stoll, J. and Lee, W. 2009. Active botnet probing to identify obscure command and control channels, Proceedings of Annual Computer Security Applications Conference (ACSAC&amp;apos;09).
- Dingbang, X. and Peng, N. 2008. Correlation analysis of intrusion alerts, Intrusion Detection Systems, Vol. 38 of Advances in Information Security, Springer US, pp. 65–92.
- Bailey, M., Cooke, E., Jahanian, F., Xu, Y. and Karir, M. 2009. A survey of botnet technology and defenses, 2009 Cybersecurity Applications Technology Conference for Homeland Security (01): 299–304. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4804459.
- Bianco, D. 2006. Detecting common botnets with snort, URL: http://blog.vorant.com/2006/03/detecting-common-botnets-with-snort.html.
- Bleeding Snort 2006. Bleeding snort website, URL: http://www.bleedingsnort.com.
- Gu, G., Porras, P., Yegneswaran, V., Fong, M. and Lee, W. 2007. Bothunter: Detecting malware infection through ids-driven dialog correlation, Proceedings of the 16th USENIX Security Symposium (Security&amp;apos;07).
- Grant, J. 2012. IRC bot source codes (written in C++, C# & Python), URL: http://darksidegeeks.com/irc-bot-source-codes-c-c-python.
- MIT Lab. 2000 DARPA intrusion detection scenario-specific datasets, URL: http://www.ll.mit.edu/mission/communications/ist/corpora/ideal/data/2000data.html.
- Lu, W., Rammidi, G. and Ghorbani, A. A. 2011. Clustering botnet communication traffic based on n-gram feature selection, Computer Communications 34(3): 502 – 514. URL: http://www.sciencedirect.com/science/article/pii/S0140366410001751.

**Index Terms**

Computer Science  
Network Security
Keywords
IRC Botnet  IRC Botnet detection  Monitoring of Network Activities  IDS alerts correlation