{tag} {/tag}

International Journal of Computer Applications

Volume 34 - Number 9

Year of Publication: 2011

Authors:

Amit Kumar Tyagi

G.Aghila

10.5120/4126-5948

{bibtex}pxc3875948.bib{/bibtex}

Abstract

Among the diverse forms of malware, Botnet is the serious threat which occurs commonly in today's cyber attacks and cyber crimes. Botnet are designed to perform predefined functions in

an automated fashion, where these malicious activities ranges from online searching of data, accessing lists, moving files sharing channel information to DDoS attacks against critical targets, phishing, click fraud etc. Existence of command and control(C&C) infrastructure makes the functioning of Botnet unique; in turn throws challenges in the mitigation of Botnet attacks. Hence Botnet detection has been an interesting research topic related to cyber-threat and cyber-crime prevention. Various types of techniques and approaches have been proposed for detection, mitigation and preventation to Botnet attack. This paper, discusses in detail about Botnet and related research including Botnet evolution, life-cycle, command and control models, communication protocols, Botnet detection, and Botnet mitigation mechanism etc. Also an overview of research on Botnets which describe the possible attacks performed by various types of Botnet communication technologies in future.

Reference

- A. Karasaridis, B. Rexroad, and D. Hoeflin, “Wide-scale Botnet detection and characterization,” in Proc. 1st Workshop on Hot Topics in Understanding Botnets, 2007.
- A. Ramachandran and N. Feamster, “Understanding the network-level behavior of spammers,” in Proc. ACM SIGCOMM, 2006.
- A. Schonewille and D. van Helmond, “The domain name service as an IDS”, Research Project for the Master System-and Network Engineering at the University of Amsterdam, 2006.
- Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna, “Your Botnet is My Botnet: Analysis of a Botnet Takeover”, 2009.
- Chao Li, Wei Jiang, Xin Zou,”Botnet: Survey and Case Study”, 4th International Conference on Innovative Computing, Information and Control, 2009.
- C. Kalt, “Internet Relay Chat: Client Protocol,” Request for Comments (RFC) 2812 (Informational), April 2000.
- 7 C. Mazzariello, “IRC traffic analysis for Botnet detection”, In Information Assurance and Security, 2008. ISIAS’08. Fourth International Conference on, pages 318–323, 2008.
- D. Dagon, G. Gu , C.P. Lee, W. Lee, “A Taxonomy of Botnet Structures,” in Proc. 23rd Annual Computer Security Applications Conference (ACSAC 2007), 2007, pp. 325-339.
- D. Dagon, “Botnet detection and response”, In OARC Workshop, 2005.
- Evan Cooke, Farnam Jahanian, Danny Mcpherson, “The Zombie Roundup, Understanding, Detecting, and Disrupting Botnets”, IEEE, 2005.
- E. Cooke, F. Jahanian, and D. McPherson, “The zombie roundup: Understanding, detecting, and disrupting botnets,” in Proc. Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI’05), 2005, pp. 39-44.
- G. Gu, J. Zhang, and W. Lee, “Botsniffer: Detecting Botnet command and control channels in network traffic,” in Proc. 15th Annual Network and distributed System Security Symposium (NDSS’08), 2008.
- G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting malware infection through ids-driven dialog correlation” In Proceedings of the 16th USENIX Security Symposium, pages 167–182, 2007.
- G. Schaffer, “Worms and Viruses and Botnets, Oh My: Rational Responses to Emerging Internet Threats”, IEEE Security & Privacy, 2006.
- H. Binsalleeh , T. Ormerod , A. Boukhtouta , P. Sinha , A. Youssef , M. Debbabi , and L.

Wang, "On the Analysis of the Zeus Botnet Crimeware Toolkit" Eighth Annual International Conference on Privacy, Security and Trust , 2010.

- H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic," in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007, pp.715-720.
- Hossein Rouhani Zeidanloo, Azizah Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei, Mazdak Zamani, "Botnet Detection Based on Traffic Monitoring" IEEE transaction,2010.
- Hossein Rouhani Zeidanloo, Azizah Abdul Manaf,"Botnet Command and Control Mechanisms", IEEE transactions, 2009.
- Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh, M. Safari, Mazdak Zamani,"A Taxonomy of Botnet Detection Techniques", 3rd IEEE Conference paper , 2010.
- Hossein Rouhani Zeidanloo, Farhoud Hosseinpour , Farhood Farid Etemad, "New Approach for Detection of IRC and P2P Botnets" , International Journal of Computer and Electrical Engineering, Vol.2, No.6, December, 2010, 1793-8163.
- The Honeynet Project. (November 7, 2007), "Know your enemy: Behind the Scenes of Malicious Web Servers" Retrieved October 31, 2009, http://honeynet.org/papers/wek/
- J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," in Proc. 1st Workshop on Hot Topics in understanding Botnets, 2007.
- Joseph Massi, Sudhir Panda, Girisha Rajappa, Senthil Selvaraj, and Swapana Revankar, "Botnet Detection and Mitigation", presented on Proceedings of Student-Faculty Research Day, CSIS, Pace University , May 7th, 2010.
- J. Binkley and S. Singh, "An algorithm for anomaly-based botnet detection" In Proceedings of USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI), pages 43–48, 2006.
- J. Goebel and T. Holz, "Rishi: Identify bot contaminated hosts by irc nickname evaluation", In USENIX Workshop on Hot Topics in Understanding Botnetsc(HotBots 07), 2007.
- K. K. R. Choo, "Zombies and Botnets," Trends and issues in crime and criminal justice, no. 333, Australian Institute of Criminology, Canberra, March 2007.
- Kapil Singh, Abhinav Srivastava, Jonathon Giffin , Wenke Lee, "Evaluating Email's Feasibility for Botnet Command and Control" International Conference on Dependable Systems &Networks: Anchorage, Alaska, June 24-27, 2008.
- Maryam Feily, Alireza Shahrestani, "A Survey of Botnet and Botnet Detection", 3rd International Conference on Emerging Security Information, Systems and Technologies, 2009.
- M. Kola, "Botnets: Overview and Case Study", PhD thesis, IBM Research, 2008.
- M. Roesch, "Snort-lightweight intrusion detection for networks", In Proceedings of the 13th USENIX conference on System administration, pages 229–238. Seattle, Washington, 1999.
- M. Akiyama, T. Kawamoto, M. Shimamura, T. Yokoyama, Y. Kadobayashi, and S. Yamaguchi, "A proposal of metrics for botnet detection based on its cooperative behavior", In Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on, pages 82–82, 2007.
- Rajab, M., Zarfoss, J., Monrose, F.,&Terzis, A. (October 2006). "A multifaceted approach to understanding the botnet phenomenon" Retrieved October 31, 2009 from

http://www.imconf.net/imc- 2006/papers/p4-rajab.pdf

- Robert F. Erbacher, Adele Cutler, Pranab Banerjee, Jim Marshall,"A Multi-Layered Approach to Botnet Detection", IEEE conference, 2010.
- Ravishankar Borgaonkar,"An Analysis of the Asprox Botnet", 4th International Conference on Emerging Security Information, Systems and Technologies, 2010.
- R.Villamarin-Salomon and J.C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic," in Proc. 5thIEEE Consumer Communications and Networking Conference (CCNC 2008), 2008, pp. 476-481.
- Ping Wang, Lei Wu, Ryan Cunningham, Cliff C. Zou," Honeypot Detection in Advanced Botnet Attacks" Int. J. Information and Computer Security, Vol. x, No. x, xxxx.
- P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic updates in the domain name system (DNS Update)," 1997, http://www.faqs.org/rfcs/rfc2136.html/.
- P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in Proc. In Workshop on Hot Topics in understanding Botnets, 2010
- Prosenjit Sinha, Amine Boukhtouta, Victor Heber Belarde, Mourad Debbabi, "Insights from the Analysis of the Mariposa Botnet"
- SANS Institute InfoSec Reading Room provided a description on "Bot & Botnet: An overview" research on topics in information security, 2003.
- Shun-Zheng Yu, Wei-Zhou Lu, "An HTTP Flooding Detection Method Based on Browser Behavior" IEEE transaction, 2006.
- Taxonomy of Botnet Threats. Trend Micro Inc. White Paper, November, 2006.
- Xuhua Ding, Wei Yu, Ying Pan,"A Dynamic Trust Management Scheme to Mitigate Malware Proliferation in P2P Networks" IEEE conference on communications, 2008.
- Xiaonan Zang, Athichart Tangpong, George Kesidis and David J. Miller, CSE Dept Technical Report on "Botnet Detection through Fine Flow Classification" Report No. CSE11-001, Jan. 31, 2011.
- Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang, Jae-Cheol Ryou, "Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention", and 2nd International Conference on Issue Date: 11-13 Aug. 2010, 2010.
- Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, K. Han, "Botnet Research Survey," in Proc. 32nd Annual IEEE International Conference on Computer Software and Applications (COMPSAC '08), 2008, pp.967- 972.
- Bot commands at http://www.viruslist.com/en/analysis?pubid=204792003
- The botnet business at http://www.securelist.com/en/analysis/204792003/The_botnet_business?print_mode=1
- Communications protocol at http://en.wikipedia.org/wiki/Communications_protocol

Index Terms

Computer Science Communications

Key words

Bot Communication protocols Honeynet

Attacks

Preventaation

Mitigation

C&C mechanism

Botnet