

## REFERENCES

- Associate, S., Hunt, P. R. and Hansman, S. (2003) *A Taxonomy of Network and Computer Attack Methodologies*.
- Barford, P. and Yegneswaran, V. (2007) ‘An Inside Look at Botnets’, in. Boston, MA: Springer US (Malware Detection), pp. 171–191.
- Bayer, U. *et al.* (2009) ‘A View on Current Malware Behaviors.’, in *LEET*.
- Bhme, R. (2013) *The economics of information security and privacy*. New York: Springer.
- Biglar Beigi, E. *et al.* (2014) ‘Towards effective feature selection in machine learning-based botnet detection approaches’, in *2014 IEEE Conference on Communications and Network Security. 2014 IEEE Conference on Communications and Network Security (CNS)*, San Francisco, CA, USA: IEEE, pp. 247–255. doi: 10.1109/CNS.2014.6997492.
- Bilge, L. *et al.* (2012) ‘Disclosure: detecting botnet command and control servers through large-scale NetFlow analysis’, in. ACM Press, p. 129. doi: 10.1145/2420950.2420969.
- Burghouwt, P. (2015) *Detection of botnet command and control traffic in enterprise networks*. TU Delft.
- Claise, B., Johnson, A. and Quittek, J. (2009) *Packet Sampling (PSAMP) Protocol Specifications*. RFC5476. RFC Editor. doi: 10.17487/rfc5476.
- Claise, B., Trammell, B. and Aitken, P. (2013) *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*. RFC7011. RFC Editor. doi: 10.17487/rfc7011.
- Cooke, E., Jahanian, F. and McPherson, D. (2005) ‘The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets’, p. 6.
- CTU-13 Dataset (2017) *Stratosphere IPS*. Available at: <https://www.stratosphereips.org/datasets-ctu13/> (Accessed: 31 August 2018).
- Ferguson, R. (2010) ‘The Botnet Chronicles A Journey to Infamy’, p. 13.
- Floor Boon, Huib Modderkolk and Steven Derix (2013) *NSA infected 50,000 computer networks with malicious software*, NRC. Available at: <https://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487> (Accessed: 14 August 2018).

François, J. et al. (2011) ‘BotTrack: Tracking Botnets Using NetFlow and PageRank’, in Domingo-Pascual, J. et al. (eds) *NETWORKING 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–14. doi: 10.1007/978-3-642-20757-0\_1.

García, S. et al. (2014) ‘An empirical comparison of botnet detection methods’, *Computers & Security*, 45, pp. 100–123. doi: 10.1016/j.cose.2014.05.011.

Giroire, F. et al. (2009) ‘Exploiting temporal persistence to detect covert botnet channels’, in *International Workshop on Recent Advances in Intrusion Detection*. Springer, pp. 326–345.

Giura, P. and Wang, W. (2012) ‘Using large scale distributed computing to unveil advanced persistent threats’, *Science J*, 1(3), pp. 93–105.

Graaf, D. D., Shosha, A. F. and Gladyshev, P. (2012) *BREDOLAB: Shopping in the Cybercrime Underworld*.

Gregory, P. (2013) *Advanced Persistent Threats for Dummies*. John Wiley & Sons.

Gu, G., Zhang, J. and Lee, W. (2007) ‘BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic’, p. 18.

Holz, T., Steiner, M., et al. (2008) ‘Measurements and Mitigation of Peer-to-peer-based Botnets: A Case Study on Storm Worm’, in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*. Berkeley, CA, USA: USENIX Association (LEET’08), pp. 9:1–9:9. Available at: <http://dl.acm.org/citation.cfm?id=1387709.1387718>.

Holz, T., Gorecki, C., et al. (2008) ‘Measuring and Detecting Fast-Flux Service Networks’, p. 12.

*ISTR, internet security report 2013* (2013). Symantec. Available at: [http://www.symantec.com/content/en/us/enterprise/other\\_resources/b-istr\\_main\\_report\\_v18\\_2012\\_21291018.en-us.pdf](http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf) (Accessed: 14 August 2018).

*ITU Botnet Mitigation Toolkit Background Information* (2008). ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector, p. 78.

J. Quittek and K. White (2006) ‘Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations’. Available at: <https://tools.ietf.org/pdf/rfc4560.pdf> (Accessed: 14 August 2018).

Martin Warmer (2011) *Detection of Web Based Command and Control Channels*. University of Twente.

Masud, M. M. et al. (2008) ‘Flow-based identification of botnet traffic by mining multiple log files’, in *2008 First International Conference on Distributed Framework and Applications*, pp. 200–206. doi: 10.1109/ICDFMA.2008.4784437.

Munoz, A. (2014) 'Machine Learning and Optimization', p. 14.

Nicolas Falliere, Eric Chien and Liam O Murchu (2011) *W32.Stuxnet Dossier*.

Symantec. Available at:

[https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf) (Accessed: 14 August 2018).

*Number of internet users 2005-2017 / Statistic* (2017) *Statista*. Available at:  
<https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>  
(Accessed: 14 August 2018).

Plohmann, D., Editors, E. G.-P. and Czosseck, C. (2012) 'Case Study of the Miner Botnet', p. 16.

Postel, J. (1981) 'DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION', p. 21.

*Protecting Your Critical Assets Lessons Learned from "Operation Aurora"* (2010). McAfee Labs and McAfee Foundstone Professional Services. Available at:  
[https://www.wired.com/images\\_blogs/threatlevel/2010/03/operationaurora\\_wp\\_0310\\_fnl.pdf](https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf) (Accessed: 14 August 2018).

Qinetiq (2014) 'Command & Control: Understanding, denying, detecting', *Qinetiq*.

Rajab, M. A. et al. (2007) 'My Botnet is Bigger than Yours (Maybe, Better than Yours)', p. 8.

Ramachandran, A. and Feamster, N. (2006) 'Understanding the Network-Level Behavior of Spammers', p. 12.

Roxburgh, A., Pawlikowski, K. and McNickle, D. C. (2004) 'Grid Computing: the Current State and Future Trends', p. 13.

Saad, S. et al. (2011) 'Detecting P2P botnets through network behavior analysis and machine learning', in. IEEE, pp. 174–180. doi: 10.1109/PST.2011.5971980.

Samuel, A. L. (1959) 'Some Studies in Machine Learning Using the Game of Checkers', p. 21.

'scikit-learn user guide' (2018).

Slonim, D. K. and Yanai, I. (2009) 'Getting Started in Gene Expression Microarray Analysis', *PLOS Computational Biology*, 5(10), pp. 1–4. doi: 10.1371/journal.pcbi.1000543.

*Spamhaus Botnet Threat Report 2017* (2017). Available at:  
<https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017>  
(Accessed: 16 August 2018).

Stevanovic, M. and Pedersen, J. M. (2014) ‘An efficient flow-based botnet detection using supervised machine learning’, in. IEEE, pp. 797–801. doi: 10.1109/ICCNC.2014.6785439.

Strayer, W. T. *et al.* (2008) ‘Botnet detection based on network behavior’, in *In Botnet Detection: Countering the Largest Security*. Springer, pp. 1–24.

Tan, P.-N., Steinbach, M. and Kumar, V. (2007) *Introduction To Data Mining*. Pearson Education. Available at:  
<http://books.google.co.id/books?id=Wx4NPK4qHXsC>.

‘The Evolution of Botnets and the Fight Against Them’ (2017). Cyren.com. Available at: [https://www.cyren.com/tl\\_files/downloads/Botnet\\_Evolution\\_Infographic.pdf](https://www.cyren.com/tl_files/downloads/Botnet_Evolution_Infographic.pdf).

Tiirmaa-Klaar, H. *et al.* (2013) ‘Botnets, Cybercrime and National Security’, in Tiirmaa-Klaar, H. et al., *Botnets*. London: Springer London, pp. 1–40. doi: 10.1007/978-1-4471-5216-3\_1.

Walton, G. (2009) *Tracking GhostNet: Investigating a Cyber Espionage Network*, p. 53.

Zheng, K. *et al.* (2016) ‘Big data-driven optimization for mobile networks toward 5G’, *IEEE Network*, 30, pp. 44–51.

Zhou, Z.-H. (2012) *Ensemble Methods*. CRC Press.

Zseby, T. *et al.* (2009) *Sampling and Filtering Techniques for IP Packet Selection*. RFC5475. RFC Editor. doi: 10.17487/rfc5475.

**SWISS GERMAN UNIVERSITY**