`Bibliography

Householder, A. Houle, K. and Dougherty, C. 2002. "Computer Attack Trends Challenge Internet Security." *CERT Coordination Center.*

Aycock, J. 2006. *Computer Viruses and Malware.*

Seifeld, C. Steenosa, R. and Welcha, I. 2009. "Capture- Behavioral analysis tool for application and documents." *The Digital Forensic Research Conference.*

Homeland Security. 2016. *Malware Trends.* National Cybersecurity and Communication Integration Center.

Khoshnaw. and Rebin B. 2017. "A comparative analysis between low and high level HoneyPots." *1st International Conference of Cihan University-Erbil on Communication Engineering and Computer Science.* Cihan University-Erbil, Kurdistan Region-Iraq.

Lee, J. 2013. *CYBER KLEPTOMANIACS: Why China Steals Our Secrets.* http://www.worldaffairsjournal.org/article/cyber-kleptomaniacs-why-china-steals-our-secrets.

Leiner, B. 2009. *A brief history of the internet.* http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Invernizzi, L. and Milani, P. 2012., "EvilSeed: A Guided Approach to Finding Malicious Web Pages." *National Science Foundation.*

Qassrawi, M. and Zhang, H. 2010. "Client Honeypots: Approaches and Challenges." *4th International Conference on New Trends in Information Science and Service Science.*

Nawrocki, M. Wahlisch, M. Schmidt, T, C. Keil, C. and Schonfelder. J. 2016. "A Survey on Honeypot Software and Data Analysis." https://arxiv.org/abs/1608.06249.

Cova, M. 2010. *Detection and Analysis of drive-by-download Attacks and Malicious Java Scripts.* University of California, Santa Barbara.

Provos, N. McNamee, D. Mavrommatis, P. Wang, K. and Modadugu, N. 2008. "The Ghost In The Browser." *Google, Inc.*

Provos, N. and Holz, T. 2007. "Virtual Honeypots: From Botnet Tracking to Intrusion Detection."

Idika, N. and Mathur, P, A. 2007. "A Survey of Malware Detection Techniques." *The 5th Conference on Information and Knowledge Technology*

Sami, S. 2011. "Hiding Virtualization from attacker." *IEEE COMPUTER SOCIETY*

Hawkins, S. Yen, D. and Chou, D. 2000. "Awareness and challenges of Internet security."
http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/HawkinsYenChou2000_IMCS8_3_AwarenessChallengesInternetSecurity.pdf.

Symantec. 2014. "Internet Security Threat Report."
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf.

Symantec. 2016. *Internet Security Threat Report.* https://infolocktech.com/wp-content/uploads/2016/04/Internet-Security-Threat-Report-ISTR-2016.pdf.

Symantec. 2015. *Internet Security Threat Report.*
https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

Symantec. 2017. *Internet Security Threat Report.*
https://resource.elq.symantec.com/e/f2.

Dumitras, T. Prakash, A and Subrahmanian. 2015. *The Global Cyber-Vulnerability Report.* Springer International.

Sun, X. 2008. "Collecting Internet Malware Based on Client Side Honeypots." *2008 The 9th International Conference for Young Computer Scientists.*

Alosefer, Y. 2012. "Analysing web-based malware behavior through Client honeypot." *Int. Journal of Engineering Research and Applications.*

Lin, Y, D. Lee, C, Y. Wu, Y, S. Ho, P, H. and Wang, F, Y. 2014. *Active versus Passive Malware Collection.* National Center for High-Performance Computing.