

## DAFTAR PUSTAKA

- [1] M. Sikorsi and A. Honig, *Practical Malware Analysis : The Hands-On Guide To Dissecting Malicious Software*, San Francisco: No Starch Press, 2012.
- [2] "APT – Advanced Persistent Threat Group – NJRAT – Historical Traffic/Indicator," [Online]. Available: <http://www.computersecurity.org/malware-traffic-samples/apt-samples/apt-advanced-persistent-threat-group-njrat-historical-trafficindicator/>. [Accessed 30 Sep 2015].
- [3] "Syrian Activists Targeted with BlackShades Spy Software," The Citizen Lab, 2012. [Online]. Available: <https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/>. [Accessed 30 September 2015].
- [4] P. Paganini, "Who and why is attacking companies in the Nordic Countries?," 2015. [Online]. Available: <http://securityaffairs.co/wordpress/37140/cyber-crime/apt-against-nordic-countries.html>. [Accessed 30 September 2015].
- [5] "Malware Analysis - Dark Comet RAT," Contextis.com, 2011. [Online]. Available: <http://www.contextis.com/resources/blog/malware-analysis-dark-comet-rat/>. [Accessed: 30- Sep- 2015. [Accessed 2015].
- [6] "Operating system market share," Netmarketshare.com., 2016. [Online]. Available: <https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. [Accessed May 2016].
- [7] A. Ismail, M. Hajjar and H. Hajjar, "Remote Administration Tools: A Comparative Study" *Journal of Theoretical and Applied Information Technology*, 2008.
- [8] Z. Chen, "Catching Remote Administration Trojan (RATs)," *SP&E*, 2000.
- [9] P. V. Ponangi, "2011," in (2011). *Cognitive Cyber Weapon Selection Tool Empirical Evaluation*, Ohio, Wright State University, 2011.
- [10] SebastianZ, "Security 1:1 - Part 2 - Trojans and other security threats," Symantec, 2015. [Online]. Available: <http://www.symantec.com/connect/articles/security-11-part-2-trojans-and-other-security-threats>. [Accessed 25 April 2015].
- [11] N. Milošević, "History of malware," *Computer Security*, 2013.
- [12] M. Sikorsi and A. Honig, *Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software*, San Francisco: No Starch Press, 2012.

- [13] S. Gadhyin and K. Bhavsar, "The Hands-On Guide to Dissecting Malicious Software," *International Journal of Advance Research in Computer Science and Software Engineering (IJARCSSE)*, 2013.
- [14] N. Bhojani, "Malware Analysis," *Confrence Paper*, DOI: 10.13140/2.1.4750.6889, 20014.
- [15] H. Carvey, *Windows Forensic Analysis Toolkit: Advanced Analysis Technique for Windows 7*, Syngress, 2012.
- [16] M. H. Ligh, *Malware Analyst's Cookbook And DVD*, IN: Wiley, 2011.
- [17] C. Eagle, *The IDA Pro Book*, 2nd ed., San Fransisco: No Starch Press, 2011.
- [18] A. Frank, "Live Forensics: Diagnosing Your System Without Killing It First," *ACM*, vol. vol 49, 2006.
- [19] G. B. Satrya, "The Detection of 8 Type Malware botnet using Hybrid Malware Analysis in Executable File Windows Operating Systems," *Proceedings of the 17th International Conference on Electronic Commerce (ICEC)*, 2015.
- [20] M. Egele, T. Scholte and dkk, "A Survey on Automated Dynamic Malware Analysis Techniques and Tools," *ACM Computing Survey*, 2011.