

## REFERENCES

Ahmadian, M. M. and Shahriari, H. R., “2entFOX: A framework for high survivable ransomwares detection,” in “Information Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on,” pp. 79–84, IEEE, 2016.

Ahmadian, M. M., Shahriari, H. R., and Ghaffarian, S. M., “Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares,” in “Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on,” pp. 79–84, IEEE, 2015.

Al-rimy, B. A. S., Maarof, M. A., and Shaid, S. Z. M., “A 0-Day Aware Crypto-Ransomware Early Behavioral Detection Framework,” in “International Conference of Reliable Information and Communication Technology,” pp. 758–766, Springer, 2017.

Amini, P., Araghizadeh, M. A., and Azmi, R., “A survey on Botnet: Classification, detection and defense,” in “Electronics Symposium (IES), 2015 International,” pp. 233–238, IEEE, 2015.

Bhardwaj, A., Avasthi, V., Sastry, H., and Subrahmanyam, G., “Ransomware digital extortion: a rising new age threat,” *Indian Journal of Science and Technology*, volume 9(14), 2016.

Bridges, L., “The changing face of malware,” *Network Security*, volume 2008(1) pp. 17–20, 2008.

Cabaj, K., Gawkowski, P., Grochowski, K., and Osojca, D., “Network activity analysis of CryptoWall ransomware,” *Przegląd Elektrotechniczny*, volume 91(11) pp. 201–204, 2015.

Cabaj, K. and Mazurczyk, W., “Using software-defined networking for ransomware mitigation: the case of cryptowall,” volume 30(6) pp. 14–20, 2016.

Chen, Q. and Bridges, R. A., “Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware,” *arXiv preprint arXiv:1709.08753*, 2017.

Gazet, A., “Comparative analysis of various ransomware virii,” volume 6(1) pp. 77–90, 2010.

Genç, Z. A., Lenzini, G., and Ryan, P., “The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware,” , 2017.

Giri, B. N., Jyoti, N., and AVERT, M., “The Emergence of Ransomware,” in “9th Annual Association of anti-Virus Asia Researchers (AVAR) International Conference—Digital Security: Prevention to Prosecution. Auckland, NZ,” Citeseer, 2006.

Gu, G., Perdisci, R., Zhang, J., Lee, W. et al., “BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection.” in “USENIX security symposium,” volume 5, pp. 139–154, 2008.

Hampton, N. and Baig, Z. A., “Ransomware: Emergence of the cyber-extortion menace,” , 2015.

Internetworldstats, “World Internet Users Statistics and 2018 World Population Stats,” , 2017.

Josse, S., “White-box attack context cryptovirology,” volume 5(4) p. 321, 2009.

Joy, J., John, A., and Joy, J., “Rootkit detection mechanism: a survey,” in “Advances in Parallel Distributed Computing,” pp. 366–374, Springer, 2011.

Kaspersky, “Kaspersky Security Bulletin: Overall Statistics for 2015,” [https://securelist.com/files/2015/12/KSB\\_2015\\_Statistics\\_FINAL\\_EN.pdf](https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf), 2015, accessed on 2017-12-05.

Kaspersky, “Kaspersky Security Bulletin: Overall Statistics for 2016,” [https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky\\_Security\\_Bulletin\\_2016\\_Statistics\\_ENG.pdf](https://kasperskycontenthub.com/securelist/files/2016/12/Kaspersky_Security_Bulletin_2016_Statistics_ENG.pdf), 2016, accessed on 2017-12-05.

Kaspersky, “Kaspersky Security Bulletin: Overall Statistics for 2017,” [https://kasperskycontenthub.com/securelist/files/2017/12/KSB\\_statistics\\_2017\\_EN\\_final.pdf](https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf), 2017, accessed on 2017-12-05.

Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., and Kirda, E., “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware.” in “USENIX Security Symposium,” pp. 757–772, 2016.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E., “Cutting the gordian knot: A look under the hood of ransomware attacks,” in “International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment,” pp. 3–24, Springer, 2015.

Kim, D., Soh, W., and Kim, S., “Design of quantification model for prevent of cryptolocker,” *Indian Journal of Science and Technology*, volume 8(19), 2015.

Kim, S., Park, J., Lee, K., You, I., and Yim, K., “A Brief Survey on Rootkit Techniques in Malicious Codes.” *J. Internet Serv. Inf. Secur.*, volume 2(3/4) pp. 134–147, 2012.

Kolodenker, E., Koch, W., Stringhini, G., and Egele, M., “PayBreak: defense against cryptographic ransomware,” in “Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security,” pp. 599–611, ACM, 2017.

Kumar, S. M. and Kumar, M. R., “Cryptoviral Extortion: A virus based approach,” *International Journal of Computer Trends and Technology (IJCTT)*, volume 4(5) pp. 1149–1153, 2013.

Kurose, J. F., *Computer networking: A top-down approach featuring the internet, 3/E*, Pearson Education India, 2005.

Liao, K., Zhao, Z., Doupé, A., and Ahn, G.-J., “Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin,” in “Electronic Crime Research (eCrime), 2016 APWG Symposium on,” pp. 1–13, IEEE, 2016.

Liao, Q., “Ransomware: a growing threat to SMEs,” in “Conference Southwest Decision Science Institutes,” , 2008.

Liska, A. and Gallo, T., “Ransomware: Defending against digital extortion,” , 2016.

Luo, X. and Liao, Q., “Awareness education as the key to ransomware prevention,” *Information Systems Security*, volume 16(4) pp. 195–202, 2007.

Luo, X. and Liao, Q., “Ransomware: A new cyber hijacking threat to enterprises,” in “Handbook of research on information security and assurance,” pp. 1–6, IGI Global, 2009.

Netmarketshare, “Operating System Market Share,” <https://netmarketshare.com/operating-system-market-share.aspx>, 2018, accessed on 2018-01-05.

Niemelä, J., “Mobile Malware And Monetizing 2011,” *Protecting the Irreplaceable, f-Secure*, 2011.

Orkhan Mamedov, Fedor Sinitsyn, and Anton Ivanov, “Bad Rabbit ransomware,” , 2017, URL <https://securelist.com/bad-rabbit-ransomware/82851/>.

Palisse, A., Le Boudier, H., Lanet, J.-L., Le Guernic, C., and Legay, A., “Ransomware and the legacy crypto API,” in “International Conference on Risks and Security of Internet and Systems,” pp. 11–28, Springer, 2016.

Pathak, N., Pawar, A., and Patil, B., “A Survey on Keylogger: A Malicious Attack,” *International Journal of Advanced Research in Computer Engineering and Technology*, 2015.

Puri, R., “Bots & botnet: An overview,” *SANS Institute*, volume 3 p. 58, 2003.

Reuters, “Two major Indonesian hospitals attacked in “Ransomware” storm,” , 2017, URL <https://www.reuters.com/article/cyber-attack-indonesia/two-major-indonesian-hospitals-attacked-in-ransomware-storm-idUSL4N1IF051>.

Richardson, R. and North, M., “Ransomware: Evolution, mitigation and prevention,” *International Management Review*, volume 13(1) p. 10, 2017.

Rudd, E. M., Rozsa, A., Günther, M., and Boulton, T. E., “A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions,” *IEEE Communications Surveys & Tutorials*, volume 19(2) pp. 1145–1172, 2017.

Saha, B. and Gairola, A., “Botnet: an overview,” *CERT-In White Paper, CIWP-2005-05*, volume 240, 2005.

Salvi, M. H. U. and Kerkar, M. R. V., “Ransomware: A cyber extortion,” *ASIAN JOURNAL FOR CONVERGENCE IN TECHNOLOGY (AJCT)-UGC LISTED*, volume 2, 2016.

Savage, K., Coogan, P., and Lau, H., “The evolution of ransomware,” , 2015.

Scaife, N., Carter, H., Traynor, P., and Butler, K. R., “Cryptolock (and drop it): stopping ransomware attacks on user data,” in “Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on,” pp. 303–312, IEEE, 2016.

Sgandurra, D., Muñoz-González, L., Mohsen, R., and Lupu, E. C., “Automated dynamic analysis of ransomware: Benefits, limitations and use for detection,” , 2016.

Sikorski, M. and Honig, A., *Practical malware analysis: the hands-on guide to dissecting malicious software*, no starch press, 2012.

Singh, Y. K., *Fundamental of research methodology and statistics*, New Age International, 2006.

Statcounter, “Desktop Windows Version Market Share Worldwide - January 2018,” <http://gs.statcounter.com/windows-version-market-share/desktop/worldwide/#monthly-201701-201801-bar>, 2018, accessed on 2018-01-05.

Tokuda, H., “Malware Detection by Process’s File Activity Monitoring,” , 2012.

WeckstÄn, M., Frick, J., SjústrÄm, A., and JÄd’rpe, E., “A novel method for recovery from Crypto Ransomware infections,” in “Computer and Communications (ICCC), 2016 2nd IEEE International Conference on,” pp. 1354–1358, IEEE, 2016.

Zavarsky, P., Lindskog, D., and others, “Experimental analysis of ransomware on windows and android platforms: Evolution and characterization,” volume 94 pp. 465–472, 2016.

Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P., and Han, K., “Botnet research survey,” in “Computer Software and Applications, 2008. COMPSAC’08. 32nd Annual IEEE International,” pp. 967–972, IEEE, 2008.