UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR PUSTAKA

[1] ENISA, “Main incidents in the EU and worldwide ENISA Threat Landscape,” 2020.

[2] A. Dulaunoy, G. Wagener, A. Iklody, S. Mokaddem, and C. Wagner, “AN INDICATOR SCORING METHOD FOR MISP PLATFORMS,” 2018.

[3] M. Maasberg, M. Ko, and N. L. Beebe, “Exploring a systematic approach to malware threat assessment,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, Mar. 2016, vol. 2016-March, pp. 5517–5526. doi: 10.1109/HICSS.2016.682.

[4] K. Ram, M. Rao, and D. Pant, “A threat risk modeling framework for Geospatial Weather Information System (GWIS): a DREAD based study,” *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 1, no. 3, 2010, [Online]. Available: http://ijacsa.thesai.org/

[5] J. Gordon, V. Kraj, J. H. Hwang, and A. Raja, “A Security Assessment for Consumer WiFi Drones,” Nov. 2019. doi: 10.1109/ICII.2019.00011.

[6] Z. Lai, Y. Shen, and G. Zhang, “A security risk assessment method of website based on threat analysis combined with AHP and entropy weight,” in *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, Jul. 2016, vol. 0, pp. 481–484. doi: 10.1109/ICSESS.2016.7883113.

[7] R. W. Saaty, “The Analytic Hierarchy Process-What it is and how it is used,” 1987.

[8] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, “MISP - The design and implementation of a collaborative threat intelligence sharing platform,” in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, Oct. 2016, pp. 49–56. doi: 10.1145/2994539.2994542.

[9] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, “Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies,” *IEEE Access*, vol. 8, pp. 124134–124144, 2020, doi: 10.1109/ACCESS.2020.3006172.

[10] ENISA, “A good practice guide of using taxonomies in incident prevention and detection,” 2016, doi: 10.2824/780536.

[11] J. Lan, “Research on Cybersecurity Risk Assessment in SCADA Networks Based on AHP-RSR,” in *Proceedings - 2020 International Conference on Communications, Information System and Computer Engineering, CISCE 2020*, Jul. 2020, pp. 361–364. doi: 10.1109/CISCE50729.2020.00079.

[12] Press OU, *Oxfprd English Dictionary*. 2013.

[13] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, “Cyber threat intelligence – Issue and challenges,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 371–379, Apr. 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.

[14] BSSN, “Indonesia Cyber Security Monitoring Report,” 2019.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[15] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24–31, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[16] G. Rasool, S. Iqbal, S. Hussain, A. Kamal, and S. Ahmad, "Threat Modelling Methodologies: A Survey," *Sci.Int.(Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014, [Online]. Available: https://www.researchgate.net/publication/307902746

[17] Musianto, "Perbedaan Pendekatan Kuantitatif dengan Pendekatan Kualitatif dalam Metode Penelitian," 2002.

[18] H. Cho, S. Lee, N. Kim, B. Kim, and J. Park, "Method of Quantification of Cyber Threat Based on Indicator of Compromise," Sep. 2018. doi: 10.1109/PlatCon.2018.8472733.

[19] Kaspersky, "Indicator of Compromise (IoC)," 2018.

[20] D. Planqué, "Cyber Threat Intelligence From confusion to clarity; An investigation into Cyber Threat Intelligence," 2017.

[21] L. Qiang, Y. Zeming, L. Baoxu, J. Zhengwei, and Y. Jian, "Framework of cyber attack attribution based on threat intelligence," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2017, vol. 190, pp. 92–103. doi: 10.1007/978-3-319-52727-7_11.

[22] MISP, "MISP-Taxonomies," 2021. https://github.com/MISP/misp-taxonomies

[23] ENISA, "Reference Incident Classification Taxonomy: Task Force Status and Way Forward," 2018. [Online]. Available: www.enisa.europa.eu

[24] J. D. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, "Threat Modeling." Jun. 2010. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

[25] H. Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7," 2012.

[26] D. Deka, N. Sarma, and N. J. Panicker, "Malware detection vectors and analysis techniques: A brief survey," in *2016 International Conference on Accessibility to Digital World, ICADW 2016 - Proceedings*, Jul. 2016, pp. 81–85. doi: 10.1109/ICADW.2016.7942517.

[27] BITS, "Malware Risks and Mitigation Report," 2011.

[28] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 925–941, 2014. doi: 10.1109/SURV.2013.070813.00214.

[29] Microsoft, "Microsoft Security Intelligence Report," 2011.

[30] D. T. Sullivan, "Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0," 2015.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[31] "Kaspersky Threats Classes." [Online]. Available: https://threats.kaspersky.com/en/class/

[32] F-Secure", "Classification Guide | F-Secure." [Online]. Available: https://www.f-secure.com/v-descs/guides/classification_guide.shtml

[33] J. Aycock, *Computer Viruses and Malware (Advances in Information Security, 22)*, 2006th ed. Springer, 2006.

[34] Monnappa. K. A, *Learning Malware Analysis : Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware.* Packt Publishing Ltd, 2018.

[35] W. Stallings, *Computer Security: Principles and Practice*, 4th ed. PEARSON INDIA, 2021.

[36] P. Janes, "People, Process, and Technologies Impact on Information Data Loss," 2012.

[37] S. Yilmaz, S. Zavrak, and Z. #2, "Adware: A Review," 2015. [Online]. Available: https://www.researchgate.net/publication/294709236

[38] S. Suresh, F. di Troia, K. Potika, and M. Stamp, "An analysis of Android adware," *Journal of Computer Virology and Hacking Techniques*, vol. 15, no. 3, pp. 147–160, Sep. 2019, doi: 10.1007/s11416-018-0328-8.

[39] L. Constantin, "What is adware? How it works and how to protect against it." Jun. 2019. [Online]. Available: https://www.csoonline.com/article/3406422/what-is-adware-how-it-works-and-how-to-protect-against-it.html

[40] J. Gao, L. Li, P. Kong, T. F. Bissyande, and J. Klein, "Should You Consider Adware as Malware in Your Study?," Feb. 2019. doi: 10.1109/SANER.2019.8668010.

[41] D. L. Prowse, *CompTIA security+ SY0-401 authorized cert guide, deluxe edition*. Pearson Education, 2015.

[42] C. Wysopal and C. Eng, "Static Detection of Application Backdoors," 2007. doi: http://dx.doi.org/10.1007/s11623-010-0024-4.

[43] Malwarebytes, "Backdoor Computing Attacks." https://www.malwarebytes.com/backdoor (accessed May 15, 2021).

[44] D. Harley, A. Lee, and C. Borghello, "Net of the Living Dead: Bots, Botnets and Zombies," 2012.

[45] S. Almutairi, S. Mahfoudh, S. Almutairi, and J. S. Alowibdi, "Hybrid Botnet Detection Based on Host and Network Analysis," *Journal of Computer Networks and Communications*, vol. 2020, 2020, doi: 10.1155/2020/9024726.

[46] S. A. Rahalkar, *Certified Ethical Hacker (CEH) Foundation Guide*. Apress, 2016. doi: 10.1007/978-1-4842-2325-3.

[47] X. Wang, L.-Y. Chen, F. Liu, and Z. Lei, "Analysis and Modeling of the Botnet Propagation Characteristics," Sep. 2010. doi: 10.1109/WICOM.2010.5601301.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[48] Techopedia", “Browser Modifier.” Jun. 2011. [Online]. Available: https://www.techopedia.com/definition/41/browser-modifier

[49] Avast Academy Team", “What is a Browser Hijacker?” [Online]. Available: https://www.avast.com/c-browser-hijacker

[50] US Norton, “What Are Browser Hijackers?” https://us.norton.com/internetsecurity-malware-what-are-browser-hijackers.html

[51] Kaspersky", “What Is Browser Hijacking?” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/browser-hijacking

[52] S. Pilici, “How to remove BrowserModifier:Win32/Prifou Virus (Removal Guide).” Jun. 2017. [Online]. Available: https://malwaretips.com/blogs/remove-browsermodifier-win32-prifou/

[53] J. Gardiner, M. Cova, and S. Nagaraja, “Command & Control Understanding, Denying and Detecting,” 2014.

[54] F-Secure, “Constructor Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/v-descs/constructor.shtml

[55] W. Han, J. Xue, Y. Wang, L. Huang, Z. Kong, and L. Mao, “MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics,” *Computers and Security*, vol. 83, pp. 208–233, Jun. 2019, doi: 10.1016/j.cose.2019.02.007.

[56] R. v. Deshmukh and K. K. Devadkar, “Understanding DDoS attack & its effect in cloud environment,” in *Procedia Computer Science*, 2015, vol. 49, no. 1, pp. 202–210. doi: 10.1016/j.procs.2015.04.245.

[57] R. Shimonski, *CEH v9: Certified Ethical Hacker Version 9 Study Guide*, 3rd ed. Sybex, 2016.

[58] M. Souppaya and K. Scarfone, “Guide to Malware Incident Prevention and Handling for Desktops and Laptops,” Gaithersburg, MD, Jul. 2013. doi: 10.6028/NIST.SP.800-83r1.

[59] S., D. Liu, S. Miller, M. Lucas, A. Singh, and J. Davis, *Firewall Policies and VPN Configurations*, 1st ed. Syngress, 2006.

[60] U. Kignuolis, “What are dialers and how to remove them.” Jun. 2017. [Online]. Available: https://www.2-spyware.com/dialers-removal

[61] Panda Security", “What is a dialer? - Panda Security.” [Online]. Available: https://www.pandasecurity.com/en/security-info/dialer/

[62] Kaspersky", “What Is BitTorrent and Is It Safe?” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/bittorrent

[63] J. C. Chen and B. Li, “Evolution of Exploit Kits: Exploring Past Trends and Current Improvements.”

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[64] A. Kurniawan, A. Fitriansyah, and L. Lppm, “What is Exploit Kit and How Does it Work?,” Jun. 2017.

[65] P. Szor, *The art of computer virus research and defense*. 2005.

[66] D., “Exploits and exploit kits - Windows security.” Jun. 2021. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware

[67] “Exploit kit Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/v-descs/exploit_kit.shtml

[68] F-Secure, “Hack-Tool Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/sw-desc/hack-tool.shtml

[69] M. Corporation, “Threat description search results - Microsoft Security Intelligence.” [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=hacktool

[70] “Hacktool.” Jun. 2019. [Online]. Available: https://blog.malwarebytes.com/detections/hacktool/

[71] Microsoft", “Hacktool - Microsoft Security Intelligence.” [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=hacktool

[72] F-Secure, “Joke Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/v-descs/joke.shtml

[73] “Monitoring-Tool Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/sw-desc/monitoring-tool.shtml

[74] V. Shanmugavel, S. Sankar, A. Kumar, M. Satheeshkumar, and S. Malathi, “Potentially Unwanted Program Analysis and Detection using YARA Rules,” *International Journal of Engineering and Advanced Technology*, vol. 9, no. 5, Jun. 2020, doi: 10.35940/ijeat.E9855.069520.

[75] A. Goretsky, “Problematic, Unloved and Argumentative: What is a potentially unwanted application (PUA)?,” 2011.

[76] “Ransomware Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/v-descs/ransomware.shtml

[77] Kaspersky", “Ransomware – definition, prevention and removal.” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware

[78] Deloitte, “Taking data hostage: The rise of ransomware.”

[79] N. Shah and M. Farik, “Ransomware-Threats, Vulnerabilities And Recommendations,” *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 6, no. 06, 2017, [Online]. Available: www.ijstr.org

[80] McAfee, “Understanding Ransomware and Strategies to Defeat it McAfee Labs.”

Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[81] A. Mohanta, M. Hahad, and K. Velmurugan, *Preventing Ransomware: Understand, prevent, and remediate ransomware attacks*. Packt Publishing, 2018.

[82] M. N. Miah, “Ransomware Attacks: Challenges and Defence.” [Online]. Available: https://hal.archives-ouvertes.fr/hal-02558819

[83] Nccic and Ics-cert, “Destructive Malware,” 2017. [Online]. Available: http://www.us-cert.gov/privacy/

[84] K. Grustniy, “Remote tech support, yet another risk factor for business.” Jun. 2019. [Online]. Available: https://www.kaspersky.com/blog/dangerous-remote-access/27538/

[85] Cyberint, “Legit Remote Admin Tools Turn Into Threat Actors’ Tools,” 2019.

[86] C. J. Dietrich, C. Rossow, and N. Pohlmann, “Exploiting visual appearance to cluster and detect rogue software,” 2013. doi: 10.1145/2480362.2480697.

[87] SC Magazine, “Rogue software The plague of rogue anti-virus,” 2010. [Online]. Available: www.scmagazineus.com

[88] M. Cova, C. Leita, O. Thonnard, A. Keromytis, and M. Dacier, “Gone Rogue: An Analysis of Rogue Security Software Campaigns.” [Online]. Available: http://www.symantec.

[89] S. Anderson, “What is Rogue Security Software and How to Protect Against it.” Jun. 2020. [Online]. Available: https://www.safetydetectives.com/blog/what-is-rogue-security-software-and-how-to-protect-against-it/

[90] Sherdian", “Information Security - Misleading Applications.” [Online]. Available: https://it.sheridancollege.ca/service-catalogue/security/misleading-apps.html

[91] McAfee, “Rootkits, Part 1 of 3: The Growing Threat,” 2006.

[92] J. Alsalam, S. Banerjee, G. Musick, and R. Saftoiu, “Computer Security and Rootkits,” 2005.

[93] “Microsoft | Malware Protection Center Threat Report: Rootkits,” 2012.

[94] M. Corporation, “Microsoft Security Intelligence.” [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=SettingsModifier

[95] S. Pilici, “Remove SettingsModifier:Win32/PossibleHostsFileHijack Adware (Guide).” Jun. 2017. [Online]. Available: https://malwaretips.com/blogs/remove-settings-modifier-win32-possiblehostsfilehijack/

[96] F-secure", “Application.Bundler Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/sw-desc/application_bundler.shtml

[97] Microsoft, “MMPC Threat Intellegence Report,” 2015.

[98] B. Lewis, I. Smith, M. Fowler, and J. Licato, “The robot mafia: A test environment for deceptive robots,” in *28th Modern Artificial Intelligence and Cognitive Science Conference, MAICS 2017*, 2017, pp. 189–190. doi: 10.1145/1235.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[99] A. Hughs, “Attack of the Spoofer,” 2018.

[100] I. Belcic and E. Farrier, “What Is Spoofing and How Can You Prevent it?,” Jun. 03, 2021. What Is Spoofing and How Can You Prevent it? (accessed Jun. 16, 2021).

[101] Kaspersky", “What is Spyware?” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/spyware

[102] A. Molnar, D. Harkin, and A. by Adam Molnar, *The Consumer Spyware Industry An Australian-based analysis of the threats of consumer spyware The Consumer Spyware Industry: An Australian-based analysis of the threats of consumer spyware*. 2019.

[103] A. Hackworth, “Spyware,” 2005.

[104] T. T. Arif Assistant, “Spyware: A Growing Software Threat.”

[105] F-Secure, “Spyware Description | F-Secure Labs.” [Online]. Available: https://www.f-secure.com/sw-desc/spyware.shtml

[106] S. Bryant, “Spyware: Causes, Effects and Prevention,” 2016.

[107] K. Wang, X. Chen, and Y. Xu, “A Brief Study of Trojan.”

[108] Z. Zhenfang, “Study on Computer Trojan Horse Virus and Its Prevention,” *International Journal of Engineering and Applied Sciences*, 2015.

[109] Kaspersky", “What is a Trojan? - Definition and Explanation.” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/trojans

[110] AVG, “What is a Trojan Horse? Is it Malware or Virus?” Accessed: Jun. 15, 2021. [Online]. Available: https://www.avg.com/en/signal/what-is-a-trojan

[111] Malwarebytes, “VirTool.” Jun. 2019. [Online]. Available: https://blog.malwarebytes.com/detections/virtool/

[112] Kaspersky, “Kaspersky Threats VirTool,” 2016. https://threats.kaspersky.com/en/class/VirTool/

[113] W. Schneider, “Computer viruses: What they are, how they work, how they might get you, and how to control them in academic institutions,” 1989.

[114] S. Bahukhandi and S. Singh Rana, “Introduction & History of Computer Viruses,” *International Journal of Scientific & Engineering Research*, vol. 7, 2016, [Online]. Available: http://www.ijser.org

[115] M. Jorge, “Editorial Note on Hazards of Computer Viruses,” vol. 14, p. 2021, 2021.

[116] R. Husain and S. Suru, “An Advance Study on Computer Viruses as Computer architecture,” *International Journal of Engineering and Technical Research*, vol. 2, no. 11, 2014.

[117] A. Tanenbaum, *Modern Operating systems*, 4th ed. Pearson India, 2016.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[118] P. P. Thakur and S. Vaidya, "The Impact of Computer Virus Attacks and its Detection and Preventive Mechanism among Personal Computer PC Users," 2015. [Online]. Available: http://typeslist.com/different-types-of-

[119] F. Syed, "Understanding Worms, Their Behaviour and Containing Them," 2009. Accessed: Jun. 02, 2021. [Online]. Available: https://www.cse.wustl.edu/%20jain/cse571-09/ftp/worms/index.html

[120] F. Adi Rafrastara and A. Pratama, "Performance Evaluation of Linear Regression Algorithm in Cluster Environment View project Computer Worm Classification," 2012. [Online]. Available: https://www.researchgate.net/publication/299580232

[121] J. Kraken, "Analysis of malware-the Morris Worm," 2019.

[122] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in *Proceedings - 2010 International Conference on Broadband, Wireless Computing Communication and Applications, BWCCA 2010*, 2010, pp. 297–300. doi: 10.1109/BWCCA.2010.85.

[123] S. Venkatachalam, "Detecting Undetectable Computer Viruses," San Jose, CA, USA, 2010. doi: 10.31979/etd.j6tm-a5pd.

[124] A. Hardikar and A. M. Hardikar, "Malware 101-Viruses," 2008.

[125] B. Bashari Rad, S. Ibrahim, and M. Masrom, "Camouflage in Malware: from Encryption to Metamorphism," *IJCSNS International Journal of Computer Science and Network Security*, vol. 12, no. 8, p. 74, 2012, [Online]. Available: https://www.researchgate.net/publication/235641122

[126] D., "Tunneling Viruses." Jun. 2013. [Online]. Available: https://www.cknow.com/cms/vtutor/tunneling-viruses.html

[127] "User mode and kernel mode - Windows drivers," *https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode*, Apr. 20, 2017.

[128] U. Mishra, "How do Viruses Attack Anti-Virus Programs," *SSRN Electronic Journal*, 2013, doi: dx.doi.org/10.2139/ssrn.2296319.

[129] W. Lee, "Malware and Attack Technologies," 2019. [Online]. Available: http://www.nationalarchives.gov.uk/doc/open-government-licence/.

[130] S. Saad, F. Mahmood, W. Briguglio, and H. Elmiligi, "JSLess: A Tale of a Fileless Javascript Memory-Resident Malware," Nov. 2019, [Online]. Available: http://arxiv.org/abs/1911.11276

[131] N. Kersh, "What is Fileless Malware?," *https://www.allot.com/blog/what-is-fileless-malware/*, Oct. 29, 2018.

[132] K., "Trojan Droppers." Jun. 2020. [Online]. Available: https://encyclopedia.kaspersky.com/glossary/trojan-droppers/

[133] C. Eckstein and R. Carbone, "Preventing data leakage: A risk based approach for controlled use of the use of administrative and access privileges," 2015.

UNIVERSITAS
GADJAH MADA
Analisis Taksonomi Insiden Pada MISP Menggunakan Pendekatan Penilaian Ancaman Kuantitatif
FADHLAN ZAKY M, Nur Rohman Rosyid S.T., M.T., D.Eng.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

[134] P. Gordon, “Data Leakage-Threats and Mitigation,” 2007.

[135] IBM Security, “Cost of a Data Breach Report 2020,” 2020.

[136] E. Software Technologies Inc, “Egress Data Loss Prevention Report 2021,” 2021.

[137] T. Holz, M. Engelberth, and F. Freiling, “Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones,” 2008.

[138] Kaspersky, “Kaspersky Enterprise Cybersecurity Point of Threat or Point of Sale: Threats Targeting PoS Terminals,” 2017. [Online]. Available: https://securelist.com/

[139] OWASP, “OWASP Top 10-2017,” 2017. [Online]. Available: https://github.com/OWASP/Top10/issues

[140] A. Johnson, K. Dempsey, R. Ross, S. Gupta, and D. Bailey, “Guide for security-focused configuration management of information systems,” Gaithersburg, MD, Oct. 2019. doi: 10.6028/NIST.SP.800-128.

[141] M. Inzimam, C. Yongle, and Z. Zhang, “An Efficient Approach towards Assessment of Zero-day Attacks,” *International Journal of Computer Applications*, vol. 177, no. 26, Dec. 2019, doi: 10.5120/ijca2019919742.

[142] Kaspersky, “What is a Zero-day Attack? - Definition and Explanation.” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

[143] Sonicwall, “Sonicwall Cyber Threat Report: Cyber Threat Intelligence For Navigating the New Business Reality,” 2021.

[144] V. Grover, “An Efficient Brute Force Attack Handling Techniques for Server Virtualization,” *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3564447.

[145] NMAP", “Host Discovery | Nmap Network Scanning.” [Online]. Available: https://nmap.org/book/man-host-discovery.html

[146] NMAP", “Detect Nmap Scans | Nmap Network Scanning.” [Online]. Available: https://nmap.org/book/nmap-defenses-detection.html

[147] Kaspersky", “Types of Malware.” Jun. 2021. [Online]. Available: https://www.kaspersky.com/resource-center/threats/malware-classifications

[148] Avira", “Avira Virus Lab.” [Online]. Available: https://www.avira.com/en/support-virus-lab