are some limitations. With the current technology, it is difficult for a computer to run more than a few virtual machines at the same time. Thus, the user can only have four downloads per instance as each file are put into separate, dedicated virtual machines to prevent one file from infecting the others.

7. Future Work

In the future, we hope to increase the number of virtual machines one computer can handle with technological advancement. In our research, we firmly believe that virtual machines can prove to be a valuable protection mechanism against malware, and this is a step in the right direction to combating malware.

References

[1] I. Khan, "An introduction to computer viruses: problems and solutions", Library Hi Tech News, vol. 29, no. 7, pp. 8-12, 2012.

[2] "Server Message Block Overview", Microsoft, 2013. [Online]. Available: https://technet.microsoft.com/en-us/library/hh831795(v=ws.11).aspx. [Accessed: 12- Nov- 2017]

[3] "PsExec - Windows Sysinternals", Microsoft, 2016. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec. [Accessed: 12- Nov- 2017]

[4] "WMIC - Take Command-line Control over WMI", Microsoft, 2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/bb742610.aspx. [Accessed: 13- Nov- 2017]

[5] S. Shackelford, "'NotPetya' ransomware attack shows corporate social responsibility should include cybersecurity", The Conversation, 2017. [Online]. Available: http://theconversation.com/notpetya-ransomware-attack-shows-corporate-social-responsibility-should-include-cybersecurity-79810. [Accessed: 13- Nov- 2017]

[6] "kill switch | Definition of kill switch in English by Oxford Dictionaries", Oxford Dictionaries | English, 2017. [Online]. Available: https://en.oxforddictionaries.com/definition/kill_switch. [Accessed: 13- Nov- 2017]

[7] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention", International Management Review, vol. 13, no. 1, pp. 10-21, 2017.

[8] A. Kharraz, "Techniques and Solutions for Addressing Ransomware Attacks", Ph.D, Northeastern University, 2017.

[9] "Windows 10 platform resilience against the Petya ransomware attack", Microsoft Secure. 2017 [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/. [Accessed: 14- Nov- 2017]

[10] M. Miller, "What Is Least Privilege & Why Do You Need It?", Beyond Trust. 2017 [Online]. Available: https://www.beyondtrust.com/blog/what-is-least-privilege/. [Accessed: 14- Nov- 2017]

[11] "Social Engineering - Definition", Kaspersky. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/social-engineering. [Accessed: 14- Nov- 2017]

[12] "Petya Ransomware | US-CERT", US-CERT, 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-181A. [Accessed: 15- Nov- 2017]

[13] N. Weaver, V. Paxon, S. Staniford, and R. Cunningham. A taxonomy of computer worms. In Proceedings of the 2003 ACM Workshop on Rapid Malcode, pages 11–18, 2003.

[14] B. Min, V. Varadharajan, U. Tupakula and M. Hitchens, "Antivirus security: naked during updates", Software: Practice and Experience, vol. 44, no. 10, pp. 1201-1222, 2013.

[15] H. Liao, C. Richard Lin, Y. Lin and K. Tung, "Intrusion detection system: A comprehensive review", Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16-24, 2013.

[16] SH Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam,(2019). Ransomware, Threat and Detection Techniques: A Review, IJCSNS International Journal of Computer Science and Network Security, 19 (2), pp. 136-146

[17] SH Kok, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, “A Review of Intrusion Detection System Using Machine Learning Approach”, in International Journal of Engineering and Research, Jan 2019.

[18] SH Kok, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, “Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm”, in Computers MDPI, vol.8, no.4, pp.79 Nov. 2019.