F. Impact Analysis based on Damage Level Category

Currently, we have classified Jigsaw, Locky, and WannaCry as CAT6, CAT7, and CAT8 ransomware, respectively. The subsequent phase of this research involves analyzing the impacts of each ransomware sample's damage level category on the victims of the ransomware attacks.

According to the damage level categorization framework, it is possible for victims to recover data affected by both the deletion and cryptographic attacks of a ransomware incident. Data lost due to the deletion attack structure can potentially be retrieved using third-party recovery tools. However, recovering data compromised by a cryptographic attack typically requires obtaining the decryption key. This can be achieved either by paying the ransom or by exploiting the decryption key generation that occurs on the host machine. Recovery is feasible for ransomware that generates encryption keys locally rather than via the attacker's Command & Control (C&C) instructions. Consequently, it is possible to recover the decryption keys for Jigsaw and WannaCry, as both ransomware samples were able to encrypt files without network connectivity. In contrast, recovery is impossible for Locky, as it does not generate encryption keys locally.

V. CONCLUSION

From the results of our analysis using tools such as Process Monitor and x64dbg, along with the categorization framework for ransomware attack damage levels, we have derived several key insights. The use of Process Monitor and x64dbg significantly enhances our understanding of ransomware behavior by providing deep insights into system activities during infection. These tools enable us to track the interactions of ransomware with the operating system, registry, and other processes.

The categorization framework we employed allows us to classify the damage levels of ransomware attacks based on both deletion attack structures and cryptographic attack structures. This framework facilitates a detailed understanding of the behavioral patterns and impacts of ransomware. Our analysis identified the damage levels of attacks from three ransomware samples: CAT8 for WannaCry, CAT7 for Locky, and CAT6 for Jigsaw. These ransomware attacks involve file deletion, file overwriting, volume shadow copy deletion, file encryption, local key generation, and potential communication with Command and Control (C2) servers.

Dynamic analysis for damage level categorization of ransomware attacks using this framework, with the aid of Process Monitor and x64dbg, has proven to be effective enough to yield accurate results with low resource requirements. However, it is important to note that Process Monitor and x64dbg were unable to detect the deletion of volume shadow copies for two out of the three ransomware samples. Future work should focus on developing new tools and methods such as using both static and dynamic analysis approach to more effectively track volume shadow copy deletion. We believe that the dynamic analysis approach, using the framework we applied, demonstrates significant effectiveness in categorizing the damage levels of ransomware attacks and analyzing the impacts of the attacks.

DATA AND COMPUTER PROGRAM AVAILABILITY

Data and program used in this paper can be accessed in the following site: https://github.com/kh4sh3i/Ransomware-Samples.

REFERENCES

[1] O. Aslan and R. Samet, "A Comprehensive Review on Malware Detection Approaches," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 6249–6271, 2020. doi: 10.1109/ACCESS.2019.2963724.

[2] A. Afianian, S. Niksefat, B. Sadeghiyan, and D. Baptiste, "Malware dynamic analysis evasion techniques: A survey," *ACM Comput Surv*, vol. 52, no. 6, Nov. 2019, doi: 10.1145/3365001.

[3] R. Sihwail, K. Omar, and K. A. Z. Ariffin, "A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis," *International Journal on Advanced Science Engineering and Information Technology*, vol. 8, pp. 4–6, 2018.

[4] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic malware analysis in the modern era—A state of the art survey," *ACM Comput Surv*, vol. 52, no. 5, Sep. 2019, doi: 10.1145/3329786.

[5] H. Zhao, M. Li, T. Wu, and F. Yang, "Evaluation of Supervised Machine Learning Techniques for Dynamic Malware Detection," *International Journal of Computational Intelligence Systems*, vol. 11, pp. 1153 – 1169, 2018.

[6] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, "Ransomware: Recent advances, analysis, challenges and future research directions," *Comput Secur*, vol. 111, Dec. 2021, doi: 10.1016/j.cose.2021.102490.

[7] S. Aurangzeb, R. N. Bin Rais, M. Aleem, M. A. Islam, and M. A. Iqbal, "On the classification of Microsoft-Windows ransomware using hardware profile," *PeerJ Comput Sci*, vol. 7, pp. 1–24, 2021, doi: 10.7717/peerj-cs.361.

[8] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms," *Journal of Telecommunications and Information Technology*, no. 1, pp. 113–124, 2019, doi: 10.26636/jtit.2019.130218.

[9] L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability," *J Cybersecur*, vol. 6, no. 1, 2020, doi: 10.1093/CYBSEC/TYAA023.

[10] T. R. Reshmi, "Information security breaches due to ransomware attacks - a systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2. Elsevier Ltd, Nov. 01, 2021. doi: 10.1016/j.jjimei.2021.100013.

[11] R. Moussaileb, N. Cuppens, J. L. Lanet, and H. Le Bouder, "A Survey on Windows-based Ransomware Taxonomy and Detection Mechanisms: Case Closed?," *ACM Computing Surveys*, vol. 54, no. 6. Association for Computing Machinery, Jul. 01, 2021. doi: 10.1145/3453153.

[12] G. McDonald, P. Papadopoulos, N. Pitropakis, J. Ahmad, and W. J. Buchanan, "Ransomware: Analysing the Impact on Windows Active Directory Domain Services," *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22030953.

[13] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Syst Appl*, vol. 190, Mar. 2022, doi: 10.1016/j.eswa.2021.116198.

[14] B. Yamany, M. S. Elsayed, A. D. Jurcut, N. Abdelbaki, and M. A. Azer, "A New Scheme for Ransomware Classification and Clustering Using Static Features," *Electronics (Switzerland)*, vol. 11, no. 20, Oct. 2022, doi: 10.3390/electronics11203307.

[15] J. H. Park, S. K. Singh, M. M. Salim, A. E. L. Azzaoui, and J. H. Park, "Ransomware-based Cyber Attacks: A Comprehensive Survey," *Journal of Internet Technology*, vol. 23, no. 7, pp. 1557–1564, 2022, doi: 10.53106/160792642022122307010.

[16] A. Zimba, Z. Wang, and M. Chishimba, "Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To," *Journal of Computer Information Systems*, vol. 61, no. 1, pp. 53–63, 2021, doi: 10.1080/08874417.2018.1564633.

Copyright Form