IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

Malware Detection in JPEG

Prof. F. S. Ghodichor[1], Prashant Kharche[2], Chaitanya Katore[3], Ajit Adavale[4], Dipkumar Prajapat[5]
Assistant Professor, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract: *Cyberattacks on people, companies, and organizations have grown in frequency. Cybercriminals are constantly searching for efficient ways to infect targets with malware in order to initiate an attack. Millions of people use images every day all throughout the world, and the majority of users think pictures to be secure for usage, however some kinds of pictures have the potential to carry a malware payload and execute detrimental acts. The main reason JPEG is the most widely used image format is because of its lossy compression. It's applied almost everyone, from small businesses to major corporations, and is present on nearly all devices (on digital cameras, cellphones, social networking, websites, etc.). Due of their reputation for being innocuous, enormous JPEG images have a lot of potential for misuse.*

Keywords: JPEG, Automatic Interpretation, Image Processing, Artificial Intelligence, Malware Detection, CNN, Deep learning

REFERENCES

[1].pp. 7–11, 2014. 2. E. S. Solutions and Q. Heal, "Quick Heal Quarterly Threat Report | Q1 2017," 2017 url:http://www.quickheal.co.in/resources/threat-reports . [Accessed: 13-june-2017].
[2]. A. Govindaraju, "Exhaustive Statistical Analysis for Detection of Metamorphic Malware," Master's project report, Department of Computer Science, San Jose State University, 2010.
[3]. M. G. Schultz, E. Eskin, and S. J. Stolfo, "Data Mining Methods for Detection of New Malicious Executables," 2001.
[4]. D. Bilar, "Opcodes As Predictor for Malware," International Journal of Electronic Security and Digital Forensics, vol. 1, no. 2, pp. 156–168, 2007.
[5]. Y. Elovici, A. Shabtai, R. Moskovitch, G. Tahan, and C. Glezer, "Applying Machine Learning Techniques for Detection of Malicious Code in Network Traffic," Annual Conference on Artificial Intelligence. Springer Berlin Heidelberg, pp. 44–50, 2007.
[6]. R. Moskovitch, D. Stopel, C. Feher, N. Nissim, N. Japkowicz, and Y. Elovici, "Unknown malcode detection and the imbalance problem," Journal in Computer Virology, vol. 5, no. 4, pp. 295–308, 2009.
[7].R. Moskovitch et al., "Unknown malcode detection using OPCODE representation," Intelligence and Security Informatics. Springer Berlin Heidelberg, vol. 5376 LNCS, pp. 204–215, 2008
[8]. I. Santos, J. Nieves, and P. G. Bringas, "Semi-supervised learning for unknown malware detection," International Symposium on Distributed Computing and Artificial Intelligence. Springer Berlin Heidelberg, vol. 91, pp. 415–422, 2011.
[9]. I. Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as representation of executables for data-miningbased unknown malware detection," Information Sciences, vol. 231, pp. 64–82, 2013.
[10]. A. Shabtai, R. Moskovitch, C. Feher, S. Dolev, and Y. Elovici, "Detecting unknown malicious code by applying classification techniques on OpCode patterns," Security Informatics, vol. 1, no. 1, p. 1, 2012.
[11]. A. Sharma and S. K. Sahay, "An effective approach for classification of advanced malware with high accuracy," International Journal of Security and its Applications, vol. 10, no. 4, pp. 249–266, 2016.
[12]. S. K. Sahay and A. Sharma, "Grouping the Executables to Detect Malwares with High Accuracy," Procedia Computer Science, vol. 78, no. June, pp. 667–674, 2016.
[13].Kaggle, "Microsoft Malware Classification Challenge (BIG 2015)" Microsoft, URL: https://www.kaggle.com/c/malware-classification , [Accessed : 10/December/2016].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

[14]. A. Sharma and S. K. Sahay, "Evolution and Detection of Polymorphic and Metamorphic Malware: A Survey," International Journal of Computer Application, vol. 90, no. 2, pp. 7–11, 2014