International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 6, Nov-Dec-2020, ISSN (Online): 2395-566X

Enhanced MalJPEG: A Novel Approachfor the Detection of Malicious JPEG Images

Nasla K, Shabna M
Dept. of Computer Science & Engineering
MGM College of Engineering and
Pharmaceutical Sciences
Valanchery, Kerala, India
naslaanees20@gmail.com,shabna.cs.mgmcet.in

***Abstract* – In recent year cyber-attacks are increased.The attackers targeting individuals, businesses and organizations. Such attacks usually result in critical harm to the organization, such as the loss and or leakage of sensitive and confidential information. Some non-executable files allow an attacker to run arbitrary malicious code on the targeted victim machine when the file is opened. Millions of people are used images for daily purpose. In some cases, some types of images can contain a malware codes and perform harmful actions. JPEG images are used by almost everyone, from individuals to large enterprises, and on various platforms;Because cyber criminals misuse JPEG image for malicious purpose. In this paper, we design a new method is named as Enhanced MalJPEG. Our system can to detect malicious JPEG images using CNN and machine learning techniques. This method extracts different features from the JPEG file structure and CNN based features from JPEG file and leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images.**

***Keywords* – CNN, Cyber- attacks, Features, JPEG, Machine learning, Malware.**

I.INTRODUCTION

In recent years, cyber-attacks against businesses and organizations have increased Such attacks aimed at organizations usually include harmful activities such as stealing confidential information, spying and monitoring an organization, and disrupting an organization's actions. Cyber attackers are continually searching for new and effective ways to launch attacks and deliver a malicious payload to victims. Some non-executable files allow an attacker to run malicious code on the targeted victim machine when the file is opened. Machine learning based methods are efficient for detecting known and unknown malicious files. JPEG (Joint Photographic Experts Group) is the one of the most popular image format because of its lossy compression. JPEG images are used by almost everyone, from individuals to large enterprises, and on various platforms.

Cyber criminals use JPEG images as an attack vector in order to deliver their malicious payload to the victim device. The capacity to distinguish malicious JPEG images has great importance as JPEG images are widely used by individuals and businesses. Existing endpoint defense solutions which are based on signatures (e.g., antivirus), can only detect known malware based on their signature database.

In this paper, we propose a novel approach for the malicious JPEG images detection system is named Enhanced MalJPEG. This system can to detect an input JPEG image is malicious or not using machine learning techniques. The proposed method features are extracted from JPEG file structure and JPEG image. Enhanced MalJPEG extracts some features from the JPEG file structure and also extract CNN [6] based features from JPEG image and leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images. This paper is organized as follows. In Section II, we presents related works based some non-executable files like docx, pdf files etc. Section III explains the proposed Enhanced MalJPEG system and in Section IV, we conclude with a summary of our contributions.

II. LITERATURESURVEY

Various studies have as of now been performed on malware disclosure in different file types for both executable and non-executable files. In this section we likely to explain some previous malware detection methods on docx, pdf files, email and an image authentication method.In literature [1], they present a novel structural feature extraction methodology (SFEM) for XML-based Office documents. SFEM extracts discriminative features from documents, based on their structure. This method is the first feature extraction methodology tailored to XML-based documents. The extracted features contribute to the

discrimination between malicious and benign documents when used in conjunction with machine learning algo- rithms. SFEM is aimed at enhancing the detection of malicious, XML-based documents. SFEM is light, fast, and high performing, meeting the security needs of today's organizations which generate, process, transfer, receive, and analyze a massive amount of documents each day (A. Cohen N. N., 2016).
In literature [2], they proposed ML-based solutions for the detection of malicious Office documents. In thisliterature they show ALDOCX, a system pointed at exact detection of new unknown malicious docx files that moreover efficiently upgrade the framework's detection capabilities over time. ALDOCX is an active learning based framework for regularly upgrading the detection model with docx files.In this paper they presenting a new Structural Feature Extraction Methodology for docx file capable of providing accurate detection of malicious docx files and also presenting the use of machine learning algorithms for the detection of malicious Microsoft Word documents based on the new SFEM(N. Nissim A. C., 2017).

In literature [8], they present ALPD, a framework that is based on active learning methods that are specially designed to efficiently assist anti-virus vendors to focus their analytical efforts. This is done by identifying and acquiring new PDF files that are most likely malicious, as well as informative benign PDF documents. These files are used for retraining and enhancing the knowledge stores.ALPD focuses on improving anti-virus frameworks by labeling those PDF files (potentially malicious or informative benign files) that are most likely to improve the detection model's performance and, in so doing, enriching the signature repository with as many new PDF malware files as possible, further enhancing the detection process. Specifically, the ALPD framework favors files that contain new content(N. Nissim A. C.-A., 2014).

In literature [3], propose a novel set of general descriptive and independent features extracted from all email components (header, body, and attachments) for enhanced detection of malicious emails using machine learning methods. The proposed features are extracted just from the email itself, based on quick static analysis; therefore, these features are independent, since the extraction process does not require an Internet connection or the use of external services or other tools, thereby meetingthe needs of real-time detection systems. Some of these features are based on the email's structure and extracted from deep within the email's body. In this literature also proposing the integrated detection rate (IDR), a new measure which helps calibrate the threshold of a machine learning classifier in order to achieve the optimal TP and FP rates.(A. Cohen, 2018).

In literature [4],they present an effective technique for image authentication which can prevent malicious manipulations but allow JPEG lossy compression. The authentication signature is based on the invariance of the relationshipsbetween discrete cosine transform (DCT) coefficients at the same position in separate blocks of an image. These relationships are preserved when DCT coefficients are quantized in JPEG compression. This authentication method can distinguish malicious manipulations from JPEG lossy compression regardless of the compression ratio or the number of compression iterations(Chang, 2001).

In literature[5], in their paper they present related vulnerabilities and malware distribution approaches that exploit the vulnerabilities of scholarly digital libraries. They evaluated over two-million scholarly papers in the CiteSeerX library and found the library to be contaminated with a surprisingly large number of malicious PDF documents. In this literature they developed a two layered detection framework aimed at enhancing the detection of malicious PDF documents, Sec-Lib, which offers a security solution for large digital libraries. Sec-Lib includes a deterministic layer for detecting known malware, and a machine learning based layer for detecting unknown malware(N. Nissim A. C., 2019).

In literature[9], they present a during run-time analysis methodology for a trusted detection of unknown malware on virtual machines (VMs). They conducted trusted analysis of volatile memory dumps taken from a VM and focused on analyzing their system-calls using a sequential-mining-method. In this literature they leveraged the most informative system-calls by machine-learning algorithms for the efficient detection of malware in widely used VMs within organizations (i.e. IIS and Email server)(N. Nissim Y. L., 2018).

In literature [10],they proposed solutions for the detection of malware in executable files using machine learning. In this paper they present a novel methodology for trusted detection of ransomware in virtual servers on an organization's private cloud. We conducted trusted analysis of volatile memory dumps taken from a virtual machine (memory forensics), using the Volatility framework, and created general descriptive meta-features. We leveraged these meta-features, using machine learning algorithms, for the detection of unknown ransomware in virtual servers. They evaluated their methodology extensively in five comprehensive experiments of increasing difficulty.This methodology is designed to protect an entire running virtual server. It isdifferent from many malware detection solutions based on static or dynamic analysis which aredesigned to analyze a single suspected file (which is provided) at a time; these solutions are notsuitable for protecting an entirerunning machine when no file is actually provided(A. Cohen N. N., 2018).

III. PROPOSED SYSTEM

The Enhanced MalJPEG is machine learning and CNN based solution for the detection of malicious JPEG images. Enhanced MalJPEG system can to detect an input JPEG image is malicious or not. In Fig. 1. Enhanced MalJPEG receives a JPEG image as input. The Enhanced MalJPEGfeature extractor and CNN based feature extractor extracts the proposed features into a vector of feature. The features are then transferred to a pre-trained machine learning-based model which outputs a classification (benign/malicious) for the input image.

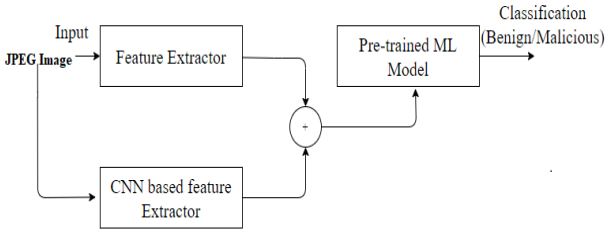

Fig. 1. Enhanced MalJPEG system

In this paper, we present Enhanced MalJPEG system for efficient detection of unknown malicious JPEG images. Enhanced MalJPEGextracts features from the JPEG file. This extracted feature leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images. Enhanced MalJPEGfeatures are extracted based on the structure of the JPEG image. EnhancedMalJPEGfeatures were defined based on an understanding of how attackers use JPEG images in order to launch attacks and how it affects the JPEG file structure in comparison to regular benign JPEG images. The features are simple and relatively easy to extract.

REFERENCES

[1] A. Cohen, N. Nissim, L. Rokach, and Y. Elovici, "SFEM: Structural feature extraction methodology for the detection of malicious office documents using machine learning methods," *Expert Syst. Appl.*, vol. 63, pp. 324–343, Nov. 2016.

[2] N. Nissim, A. Cohen, and Y. Elovici, "ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 3, pp. 631–646, Mar. 2017.

[3] A. Cohen, N. Nissim, and Y. Elovici, "Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods," Expert Syst. Appl., vol. 110, pp. 143–169, Nov. 2018.

[4] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Trans. Circuits Syst. Video Technol., vol. 11, no. 2, pp. 153–168, 2001.

[5] N. Nissim, A. Cohen, J. Wu, A. Lanzi, L. Rokach, Y. Elovici, and L. Giles, "Sec-Lib: Protecting Scholarly Digital Libraries from Infected Papers Using Active Machine Learning Framework.," IEEE Access, pp. 1–1, 2019.

[6] https://towardsdatascience.com/wtf-is-image-classification-8e78a8235acb

[7] https://www.wikipedia.org/

[8] N. Nissim, A. Cohen, R. Moskovitch, A. Shabtai, M. Edry, O. Bar-Ad, and Y. Elovici, "ALPD: Active learning framework for enhancing the detection of malicious PDF files," in Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014, 2014, pp. 91–98.

[9] N. Nissim, Y. Lapidot, A. Cohen, and Y. Elovici, "Trusted system-calls analysis methodology aimed at detection of compromised virtual machines using sequential mining," Knowledge-Based Syst., vol. 153, pp. 147–175, 2018.

[10] A. Cohen and N. Nissim, "Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory," Expert Syst. Appl., vol. 102, pp. 158–178, Jul. 2018.

About Author

Nasla K received the B.Tech degree in Computer Science and Engineering from University A P J Abdul Kalam Technological University, Kerala, India, in 2019. Presently, she is doing her Post Graduation in the Department of Computer Science and Engineering, at MGM College of Engineering and Pharmaceutical Sciences, Valanchery, Kerala. Her latest research include Cyber Security, Mobile and Computer Security ,Artificial Intelligence, Image processing and Machine Learning.

Shabna M obtained her Bachelor's degree in Computer Science and Engineering from Cochin College of Engineering and Technology, Valanchery, Kerala, India in 2016 and Master's degree in Computer Science and Engineering from Cochin College of Engineering and Technology, Valanchery, Kerala, India in 2018. Currently, she is working as Assistant Professor in the department of Computer Science and Engineering MGM College of Engineering and Pharmaceutical Sciences, Valanchery, Kerala, India. Her current research include Artificial Intelligence, Machine learning and Natural language Processing and Information Retrieval