International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/IJSRCSEIT

JPEG Vigilant : AI-Powered Malware Image Detection

Prof. J. N. Ekatpure, Nilesh Kharade, Digvijay Korake, Dipak Kshirsagar, Rushikesh Mind

Department of Computer Engineering, S. B. Patil College of Engineering, Indapur, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 Oct 2023

Published: 30 Oct 2023

Publication Issue

Volume 9, Issue 10

September-October -2023

Page Number

66-70

ABSTRACT

Cyberattacks against people, companies, and organizations have risen in recent years.In order to conduct an attack, cybercriminals are constantly searching for efficient channels to spread malware to targets. Millions of people use photos every day, and the majority of consumers believe that they are safe to use. However, some types of images may contain malicious payloads that carry out dangerous functions. Due in large part to its lossy compression, JPEG is the most widely used image for mat.In this study, we introduce JPEGVigilant, the first machine learning-based method designed exclusively for the quick and accurate identification of unknown malicious JPEG images. In order to distinguish between benign and malicious JPEG images, JPEGVigilant statically derives 10 straightforward yet discriminative properties from the JPEG LE structure.

Keywords: Machine learning, malware, detection, JPEG, image, features.

I. INTRODUCTION

to Cyber assaults often involve damaging actions like stealing sensitive data, snooping, or monitoring and affect the target (sometimes significantly). Attackers could be spurred on by ideology, criminal purpose, a need for attention, etc. Attackers are always looking for innovative and efficient ways to initiate assaults and deliver a harmful payload to targets. Frequently, this has been done through sending files over the Internet. Attackers are increasingly employing non-executable files, such as.pdf and.docx, which are incorrectly thought to be safe to use by most users, as executable files (.exe) are recognized to be harmful. Some non-executable les enable an attacker to launch arbitrary malicious code when the le is opened on the computer of the intended victim. The most widely used picture format is JPEG (Joint Photographic Experts Group), mostly due to its lossy compression. everyone uses JPEG photos, from little businesses to major corporations, and on a variety of platforms. Computers (personal photos, papers), gadgets (smartphones, digital cameras, etc.), and the internet all include JPEG images.

II. LITERATURE SURVEY

Sr. No	PaperTitle	Author	Year	Problem solved in this paper: Existing Problem Statement	Technique used to solve problem : Existing Problem Solution	Whatwillbefuturework:FutureScope
1	ANovelMachineLearning ApproachforMalwareDetection	Tarun Kumar, Sanveev Sharma, Himansh-u Goel, Sumit Chaudha-ry, Parag Jain	2019	This studyANovelMachineLearningApproachforMalware Detec-tion.	We have proposed a frame-work for malware analysis based onsemiautomatedmal-waredetectionusuallymachinelearning which is based on dynamic malware detection.	Improve accu-rancy.
2	Detection of Advanced Malware by Machine Learning TechNiques	SanjaySharma,C. RamaKrishnaandSanjay K.Sahay	2019	This studyDetection of Advanced MalwarebyMachineLearningTechniques.	We study the frequency of op-codeoccurrencetodetectunknownmalwarebyusingmachinelearningtechnique.	Infuture, wewill implement proposedapproach on dif-ferentdatasetsand will performinthedeepanalysisfortheclassificationofadvancedmalicioussoftware.
3	Novel active learning methods for enhanced PC malware detection in windows OS	NirNissim,RobertMoskovitch - Rokach,YuvalElovici	2019	WestudyNovelactivelearningmethodsfor enhancedPC malwaredetec- tion in windowsOS	In this paperweproposedaframework basedon new active1274 learningmethods (Ex-ploitation andCombination)designed for1275 acquiring unknownmalware.	Infuturework,weareinterestedin implementingthis frame-1361workalsoonAndroid appli-cations whereitisnotveryfeasible to 1362applyadvanceddetectiontech-niques over thedevice itselfdue to 1363 itsresourcelimi-tations(CPU,battery,etc.).
4	Trust Sign: Trusted Malware Signature Generation in Private	DanielNah-mias,AviadCohen,NirNissim,YuvalElovicia	2019	ToobtainanddevelopeTrust-Sign:TrustedMalwareSigna-ture	This paperpresentsTrust-Sign,anovel,trustedautomaticmalwaressignature	Firstdirectionforfutureworkisrelatedtomaintainingtheupdatability and efficiencyofourproposedsolution.

	Clouds Using Deep Feature Transfer Learning.			Generationi n Private Clouds Using DeepFeature TransferLear n-ing..	generationmethodb asedonhigh-level deepfeaturestrans-ferredfromaVGG-19neuralnetworkm odel pretrained ontheImageNet dataset.	
5	Keeping pace with the creation of new malicious PDF files using an active learn based detection framework.	NirNissim,AviadCohe n,RobertMoskovitch , AsafShabtai,MatanEd ri, O. Baradand Y. Elovici	2 0 1 9	To developeKee ping pacewith the cre-ation of newmalicio us PDFfiles using anactive-learningbase ddetectionfr amework.	In this studywe present anactive learning(AL) basedframework,sp ecificallydesigned to efficiently assistanti-virusvendorsfocust heiranalyticaleffort s imedatacquiringno velmaliciousconten t.	Infuturework,inadditiont oadditionaltypesofmalici ousdocumentswearei nterested In extendingthisframework to Androidapplications.
6	ANovelMa-chineLearn-ing Ap-proachforM al-wareDetec-tion	TarunKu-mara,SanjeevShar-maa,Himan-shuGoela,SumitChaud -harya	2 0 1 9	Toobtainand develope ANovel Ma-chineLearni ngApproach forMalware Detec-tion	In this paper, wehave proposedaframewo rkformalwareanaly -sis based on semiautomatedmal-waredetectionusual lymachinelearning whichisbasedondy-namicmalware detection.	Improvingaccu-racy.
7	Surveyof Ma-chineLearn-ing Tech-niquesforM al-wareAnaly-sis	DanieleUcci,Leonardo Aniello,RobertoBaldo ni	2 0 1 8	Tostudy Sur-veyofMachi neLearningT ech-niquesforMa l-wareAnalysi s.	This survey aimsatprovidingano verviewontheway machinelearningha sbeen used so farin the context ofmalwareanaly-sisinWindowsenvir onments.	Thenovelcon-cept of malwareanalysis eco-nomics canencourage fur-ther researchdirections,where appropriatetuningstrateg ies canbeprovidedtobalancec om-petingmetrics(e.g.accura cyandcost)whendesignin g a mal-ware analysis environment.
8	DynamicMa l-wareAnal-ysis in	Ori or- meir, Nir nis-sim, Yuval Elovici, And Lior Rokach	2 0	To study Surveyof Dynamic	Wedescribetheadva ncementsmadeinan alysistechniques	futureresearchstemsfrom thefactthatdy-namicanalysisproducesat

	theModern Era— AStateofthe ArtSurvey.		19	Mal-ware AnalysisintheModernEra— AStateofthe ArtSurvey.	dur-ing this time.Early researchcentered on functioncallanalysis,execu-tioncontrol,andflowtracking.	imesequence outputof observedbehavior.
9	DynamicMal-wareAnal-ysis in theModern Era— AStateofthe ArtSurvey	Nirnissim,aviadcohen1,jianwu,andrealanzi,liorrokach,Yuvalelovicciand leegiles	2019	To study Surveyof Dynamic Mal-ware AnalysisintheModernEra— AStateofthe ArtSurvey.	Inthisstudy,wepresent relatedvulnerabilitiesand malwaredistributionapproachesthatexploitthevulnerabilities ofscholarlydigitallibraries.	Infuturework,we suggestevaluatingthemaliciousPDFpresenceinad-ditionaldigitallibraries suchas MAS, WebofScience,andPubMed, as wellasinvestigat-ingthemforvulnerabilities.
10	MalwareDetec-tion onByteStreamsofPDFFilesUsingConvo-lutionalNeuralNet-works.	Young-SeobJeong,JiyoungWoo ,andAhReumKang	2018	To study Surveyof Malware De-tectiononByteStreamsof PDFFiles Using Con-volutionalNeu-ralNetworks.	In this paper,we design aconvolutionalneural networkto tackle themalware detec-tiononthePDFfiles. We collectmalicious andbenignPDFfiles and manuallylabel the bytesequenceswithin thefiles.	Asafuturework,wewillcollect dataofotherfiletypes (e.g.,.rtffiles)andperform furtherinvestigation.

III.LIMITATIONS OF EXISTING WORK

a) Machine learning methods have not been used particularly for the detection of malicious JPEG images.

b) Addressing these limitations requires ongoing research and development to improve the robustness, accuracy, and applicability of machine learning-based solutions for detecting malicious JPEG images.

IV.CONCLUSION

We present JPEGVigilant, a machine learning based solution for efficient detection of unknown malicious JPEG images. To the best of our knowledge, we are the first to present a machine learning-based solution tailored specifically for the detection of malicious JPEG images. JPEGVigilant extracts 10 simple but discriminative features from the JPEG le structure and leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images. JPEGVigilant features are extracted based on the structure of the

JPEG image. JPEGVigilant features were defined based on an understanding of how attackers use JPEG images in order to launch attacks and how it affects the JPEG le structure in comparison to regular benign JPEG images.

V. REFERENCES

[1]. T. Kumar, S. Sharma, Goel, S. Chaudhary, and P. Jain. A Novel Machine Learning Approach for Malware Detection. Accessed: 2019. [Online]. Available:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3383953

[2]. S. Sharma, C. R. Krishna, and S. K. Sahay, ``Detection of advanced malware by machine learning techniques,'' in Soft Computing: Theories and Applications. Singapore: Springer, 2019, pp. 333342.

[3]. N. Nissim, R. Moskovitch, L. Rokach, and Y. Elovici, ``Novel active learning methods for enhanced PC malware detection in windows OS,'' Expert Syst. Appl., vol. 41, no. 13, pp. 58435857, Oct. 2014.

[4]. D. Nahmias, A. Cohen, N. Nissim, and Y. Elovici, ``TrustSign: Trusted malware signature generation in private clouds using deep feature transfer learning,'' in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2019,pp. 18.

[5]. N. Nissim, A. Cohen, R. Moskovitch, A. Shabtai, M. Edri, O. Bar-Ad,and Y. Elovici, ``Keeping pace with the creation of new malicious PDF les using an active-learning based detection framework,'' Secur. Inform., vol. 5, p. 1, Dec. 2016.

[6]. T. Denemark, P. Bas, and J. Fridrich, ``Natural steganography in JPEG compressed images,'' Electron. Imag., vol. 2018, no. 7, pp. 316-1316-10, Jan. 2018.

[7]. D. Ucci, L. Aniello, and R. Baldoni, ``Survey of machine learning techniques for malware analysis,'' Comput. Secur., vol. 81, pp. 123147,Mar. 2019.

[8]. O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, ``Dynamic malware analysis in the modern eraA state of the art survey,'' CSURACMComput. Surv., vol. 52, no. 5, pp. 148, Sep. 2019.

[9]. 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, vol. 7,pp. 110050110073, 2019.

[10]. Y.-S. Jeong, J. Woo, and A. R. Kang, ``Malware detection on byte streams of PDF les using convolutional neural networks,'' Secur. Commun. Netw., vol. 2019, pp. 19, Apr. 2019.