lsss

by Ls Ls

Submission date: 21-Jan-2022 11:46AM (UTC+0500)
Submission ID: 1745272035
File name: Literature_servey.docx (20.53K)
Word count: 1519
Character count: 8809

The ability to see ransomware as a colored picture is a significant step forward in the malware categorization process. The concept of displaying ransomware as colored pictures was initially proposed by Nataraj et al. in [1]. Who displayed ransomware like a gray-scale picture with in domain of [0, 255], with 0 representing dark black and 255 representing full white. They noticed that the photos they acquired included multiple portions, each of which indicated distinct details about the infection. For categorization, they employed GIST to calculate texture characteristics from ransomware pictures and K-nearest neighbors.

When it comes to Deep learning, It has achieved significant progress in a variety of fields, including image identification, voice recognition, text classification, and others [2].

Syed et al. [3] suggested a ransomware variations identification approach based on infection specimen behavior; the key step was seeking evidence on malicious behavior sequences. The behavior of malware samples was acquired using their approach, which involved operating these in a simulated world.

For ransomware variant categorization, EulGyuim et al. [4] proposed a chart similarity method. His process began by converting section data from ransomware code into grey scale photos, which were then used to produce entropy charts. For chart resemblance, they employed the Strelkov entropy similarity measurement approach. Using 1000 samples spanning 50 distinct ransomware families, they were able to reach a 97.9% similarity ratio. Their approach can process a huge proportion of unpacked ransomware binary samples quickly. However, authors expressly stated in the constraints portion of their study that calculating similarity for packaged ransomware binary examples using entropy charts is a challenging process.

Viruses, Worms, Trojans, and Backdoors are all types of malware that have different capabilities. Based on the nature of variations, these categories are more divided into groups. To avoid being caught, malware authors use a variety of evasion techniques like dead-code implantation, subroutine rearrangement, and code substitution to generate variations of an existing malware group [5].

When we talk about Malware we came to that it's a malicious software that is created with the goal of damaging the computer systems.[7]

Graphics based assessment of information security assaults has recently been used in research investigations [8]. The graphical inspection of secure shell (SSH) brute-force attack efforts, which were recognised by colours for the numerous irregularities found, as well as the specifics of User IDs and Internet-Protocol (IP) addresses [9], was one semi-automated approach. Visualization methods were also used to show a huge data packets in one go. These graphics depict the connections among packet headers, allowing security experts to focus in on specifics [10]. Another research [11] employed image-based research to describe the timeline of a malicious assault like a phishing scam, with colours showing which types of system connection was effective.

In context of malware categorization, Bensaoud et al. [12] utilised 6 deep learning algorithms. VGG16, Inception V3, and ResNet50 are prior champions of ISVLVRC challenge, while the ramaining 3 algorithms are CNN-SVM, GRU-SVM, and MLP-SVM, which use Support Vector Machine (SVM) to improve neural networks. Researchers used the Malimg data for training all of the algorithms, and at the end findings show that the Original conception V3 model had the highest precision of 99.24 percent of all the research they performed at.

Naeem et al. [13] used a DCNN algorithm to transform APK data into colour pictures. Also on Leopard Mobile malware dataset3, the classifier was 97.81 percent accurate, while running on a windows dataset, it was 98.47 percent accurate.

Mercaldo and Santone [14] suggested a framework for employing guided deep learning for the identification of dangerous samples in a definite way. Researchers used a collection of attributes extracted from coloured photos to create various algorithms that could identify each virus category and variation within it. The group detection method had a 93.50 percent prediction performance, whereas variety detection method had a 95.80 percent accuracy rate.

Here are some techniques on the basis of malware pictures and deep learning:

While standard machine learning approaches have certain drawbacks, ransomware categorization relying on malware pictures plus deep learning had emerged as a viable alternative because that removes a significant amount of features engineering task.

Malware categorization using deep learning had grown increasingly appealing in the last 2 years. In malware picture categorization, Yue [15] presented a deep cnn with scaled softmax cost. According to their findings, the new error rate may be used to adapt other common convolutional neural networks and increase classification accuracy. Ni et al. [16] introduced the MCSC ransomware classification system, which used simhash to transform deconstructed malware coding into grey pictures then using a convolutional neural network for identify their groups. Kalash et al. [17] also presented a CNN-based virus categorization framework.

This approach obtained great accuracy by utilizing VGG16's before-training algorithms. Rezende et al. [18] applied the ResNet-50 design for spam filtering using deep learning too. The cnn layers of ResNet-50 pre-trained upon that ImageNet dataset were frozen to train the dnn. Gibert et al. [19] introduced a format independent deep learning strategy for ransomware categorization containing a collection of discriminating sequences generated from ransomware photos, inspired from the visual resemblance amongst ransomwares from the same groups.

Bhodia et al. [20] compared photo transfer learning-based malware detection to KNN, a basic machine learning technique. In a virtual zero-day test, the findings revealed that the approach is relies on picture transfer learning outperformed KNN.

Techniques based on Static Features:

Features which are static, they are derived from a section of a programme that does not need to be run. Static characteristics for malware detection include byte sequencing, opcode sequencing, Application Programming Interface (API), and Function Call Graph (FCG). Drew et al [21] suggested a byte sequence-based virus classification approach. The Strand (Super Threaded Reference-Free Alignment-Free Nsequence Decoder) classifier receives the malware's generated bytes patterns as input. Zhang et al. suggested a malware classification approach which is based upon n-gram patterns of opcodes [22]. The feature extraction used in this technique is the n-gram Term Frequency (TF) value composition matrix, that is used in combination of machine learning algorithm to categorise malware.

[1] Nataraj, L., Karthikeyan, S., Jacobs, G. and Manjunath, B.S. Malware Images.

[2] Yann LeCun, Yoshua Bengio and Geoffrey Hinton, "Deep learning", *nature*, vol. 521, no. 7553, pp. 436, 2015.

[3] S.Z.M. Shaid, M.A. Maarof Malware behaviour visualization J. Teknol. (2014)

[4] Alex Krizhevsky, Ilya Sutskever and E. Hinton Geoffrey, "ImageNet Classification with Deep Convolutional Neural Networks", *International Conference on Neural Information Processing Systems (NIPS)*, 2012.

[5] A. Shabtai, R. Moskovitch, Y. Elovici, C. Glezer Detection of malicious code by applying machine learning classifiers on static features: a state-of-the-art survey, Inf. Secur. Tech. Rep. (2009)

[6] K. Rieck, P. Trinius, C. Willems, T. Holz, Automatic analysis of malware behavior using machine learning, J. Comput. Secur. (2011), 10.3233/JCS-2010-0410, Google Scholar

[8] H. Shiravi, A. Shiravi, A. Ghorbani

A survey of visualisation systems for network security
IEEE Trans Vis Comput Graph, 18 (8) (2012), pp. 1313-1329

[9] WB. Balakrishnan, **Security data visualization**, SANS Institute Inc (2014)

[10] TY. Zhang, XM. Wang, ZZ. Li, F. Guo, Y. Ma, W. Chen
A survey of network anomaly visualisation
Sci China Inform Sci, 60 (12) (2017), Article 121101

[11] W. Shanks, Enhancing intrusion analysis through data visualization SANS Institute,Inc (2015)

[12] Bensaoud A., Abudawaood N., Kalita J.
Classifying malware images with convolutional neural network models
Int J Netw Secur, 22 (2020), pp. 1022-1031

[13] Naeem H., Ullah F., Naeem M.R., Khalid S., Vasan D., Jabbar S., Saeed S.
Malware detection in industrial internet of things based on hybrid image visualization and deep learning model
Ad Hoc Netw (2020), Article 102154

[14] Mercaldo F., Santone A.
Deep learning for image-based mobile malware detection
J Comput Virol Hacking Tech (2020), pp. 1-15

[15] S. Yue

Imbalanced Malware Images Classification: a cnn Based Approach, Cornell University Library (2017), pp. 1-6

[16] S. Ni, Q. Qian, R. Zhang
Malware identification using visualization images and deep learning
Comput. Secur., 77 (2018), pp. 871-885

[17] M. Kalash, M. Rochan, N. Mohammed, N.D. Bruce, Y. Wang, F. Iqbal
Malware classification with deep convolutional neural networks
2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE (2018), pp. 1-5

[18] E. Rezende, G. Ruppert, T. Carvalho, F. Ramos, P. De Geus
Malicious software classification using transfer learning of resnet-50 deep neural network
2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE (2017), pp. 1011-1014

[19] D. Gibert, C. Mateu, J. Planes, R. Vicens
Using convolutional neural networks for classification of malware represented as images
J. Comput. Virol. Hack. Tech., 15 (1) (2019)

[20] Bhodia et al. (2019) compared photo transfer learning-based malware detection to KNN, a basic machine learning technique. In a virtual zero-day test, the findings revealed that the approach is relies on picture transfer learning outperformed KNN.

[21] J. Drew, T. Moore, M. Hahsler
Polymorphic malware detection using sequence classification methods
Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016 (2016), pp. 81-87

[22] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, A.K. Sangaiah
Classification of ransomware families with machine learning based on n-gram of opcodes
Future. Gener. Comp. Sy., 90 (2019),

Isss

ORIGINALITY REPORT

8%	4%	7%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mao Xiao, Chun Guo, Guowei Shen, Yunhe Cui, Chaohui Jiang. "Image-based malware classification using section distribution information", Computers & Security, 2021 Publication	3%
2	repository.tudelft.nl Internet Source	2%
3	Submitted to University of East London Student Paper	1%
4	Sitalakshmi Venkatraman, Mamoun Alazab, R. Vinayakumar. "A hybrid deep learning image-based analysis for effective malware detection", Journal of Information Security and Applications, 2019 Publication	1%
5	Edmar Rezende, Guilherme Ruppert, Tiago Carvalho, Fabio Ramos, Paulo de Geus. "Malicious Software Classification Using Transfer Learning of ResNet-50 Deep Neural Network", 2017 16th IEEE International	1%

Conference on Machine Learning and Applications (ICMLA), 2017
Publication

6	undraderaconterschlieen.com Internet Source	1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		