Malware Detection Using Image Visualization and Deep Learning

***Saksham Tyagi**

Meerut Institute of Engineering and Technology, C.S. Dept.

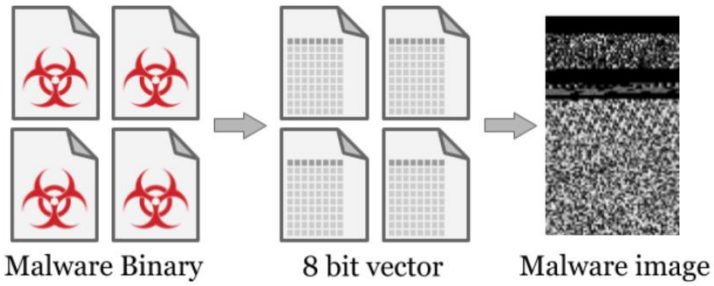
Abstract: Despite the relentless efforts of cyber security research to protect against malware threats, malware developers discover new ways to avoid these defense techniques. Usual machine learning approaches that train a classifier based on handcrafted features are not sufficiently potent against the new evasive techniques and require more efforts due to feature-engineering. We propose a visualization-based method, where malware binaries are depicted as images to successfully distinguish between malware files and clean files using a deep learning model.
Extensive experiments performed on Malimg dataset shows the accuracy to improve up to 96.97 percent.

Introduction

Malware refers to a variety of unwanted software designed to infiltrate a computer system without the owner's consent. They are categorized into different groups such as Viruses, Trojans, Botnets, Worms, Spyware and Backdoors with respect to their specifications as well as purpose [1]. Malware has been employed as the main weapon of cyber criminals to accomplish diverse security attacks, for example, gaining access to a private system, stealing user's personal information and damaging files on system, which deliver drastic damages and substantial financial loss to users. The growing number and complexity of malware have become one of the most biggest cyber security threats [2,3].Malware detection through regular signature based methods [4] is becoming non-viable since all current malware applications tend to have various polymorphic layers to evade detection or to use side mechanisms to automatically update themselves to a newer version at short periods of time in order to evade detection by any antivirus software. To address this problem, intelligent malware detection approaches are proposed. The intelligent malware detection approach uses machine learning or data mining methods to detect malwares but typical machine learning approaches that train a classifier based on handcrafted features are also not sufficient against these evasive techniques and require more efforts due to feature-engineering. To resolve these challenges, we adopted a visualization-based method, where all the malware binaries are depicted as two-dimensional images and classified using a deep learning model.
We use this method as Image visualization helps to reduce feature engineering and deep learning shows better results in image classification. To do this we will first show how to get malware images from malware. At the next step we will show the deep learning that is used to classify malware images and the last step we will show our experiment results.

Visualization of Malware

Visualization of malware has been recently used as a new and efficient technique for research in malware detection. To Visualize we make gray images from the files. In a gray image each pixel has a value from 0 to 255. When we make a gray image from a file, we read every 8 bits and convert it to an integer corresponding to a pixel. Then, we get a 256x256 image. The image size is 64KB. When the file is greater than 64KB, the remainder is discarded. When it is less than 64KB, the remainder of the image is padded with zero. In addition, when we use 256x256 images in deep learning, it runs out of memory. So, we down-sample the images to 32x32 images. Following is an image regarding converting benign files and malware into images.

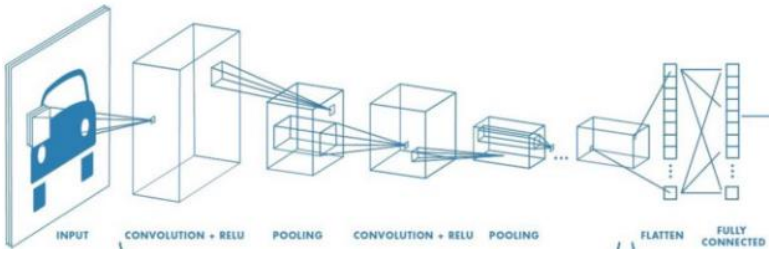


The idea that to detect malware, we can make images from benign files and malware is from [5]. The idea is that a variant of malware have similar image and different malware have different image. For this research we will use Mailmg data which is a preexisting binary pattern substantially reused to achieve variations, generating new patterns.

Deep learning

In this section, we introduce a deep learning model for malware detection using malware image. Deep learning is a specialism of machine learning, which learns the input at multiple levels to get better knowledge representations. Progress in computer vision with deep learning was developed, mainly through Convolutional Neural Networks (CNN).Deep learning is widely used in image recognition. Especially convolutional neural network (CNN) is mainly used. In neural network, each node in the previous layer gives effects to all nodes in the next layer. However, in CNN, only several nodes in the current layer give effects to the nodes in

the next layer. So, CNNs are able to use local correlation. It means that CNN learns features from the images. The following figure shows Basic CNN model



Our proposed CNN model contains 13 convolution layer each followed by Batch Normalization and pooling after every 2 layers. Our model has a dropout of 15 percent and has activation set as 'Relu'.

Result

The dataset Mali_mg was used for our proposed method. The dataset contains 23,125 images. We divided the data in 8:1:1 ratio for training, testing and validation .The experiments were performed for multiple input binary image sizes such as 32 × 32 dimensions and 64 × 64 dimensions. The results show that the information is retained and showed better predictive accuracy for images reshaped to 64 × 64

There are four types of metrics assessed to get the classification predictions.

True Positive (TP): this prediction shows that an observation belongs to a class and it actually does belong to that class, i.e., the binary image that is classified as malware and is really a malware.

True Negative (TN): this prediction shows that an observation does not belong to a class and it actually does not belong to that class, i.e., a binary image that is classified as not malware (negative) and is really not malware (negative).

False Positive (FP): this prediction shows that an observation belongs to a class and it actually does not belong to that class, i.e., a binary image that is classified as malware and is really not malware (negative).

False Negative (FN): this prediction shows that an observation does not belong to a class and it actually does belong to that class, i.e., a binary image that is classified as not malware (negative) and is really malware.

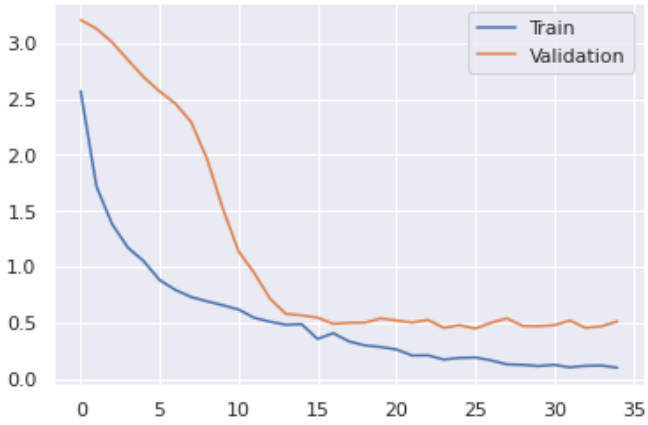
The four metrics are given below

True Positive	894
True Negative	22173
False Positive	27
False Negative	31

Accuracy (Acc), Precision (Pr), Recall and (Re) are the three main classification metrics. The number of right predictions divided by the total number of predictions can be termed as accuracy. It is defined as

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

The accuracy of our proposed model is **96.97**. The training and test loss for the given data is



The training and test accuracy for the given data is

Conclusion

In this paper, we introduce a method to detect malware using malware image and deep learning. First, we show how to generate images from benign files and malware since every variant of malware hasa similar image with the malware. Also, The images come fast compared to API sequences. Second, by using deep learning model based on CNN, we detect malware since CNN model learns features from the images. In our proposed experimental results, the accuracy is about 96.97%. In the future, we can use other pre processing methods to detect malware as well as malware images. We can use API system call sequences by doing dynamic analysis or use opcodes by doing static analysis.

Refrences

1. Bazrafshan, Z., Hashemi, H., Fard, S. M. H., et al.: 'A survey on heuristic malware detection techniques'. In The 5th Conf. on Information and Knowledge Technology, Shiraz, Iran, 2013, pp. 113–120.
2. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 2014, 80, 973–993. [CrossRef]
3. Amoroso, E. Recent progress in software security. IEEE Softw. 2018, 35, 11–13. [CrossRef]
4. I. Santos, Y. K. Penya, J. Devesa, and P. G. Garcia, "N-grams-based file signatures for malware detection," 2009
5. L.Nataraj, Malware Images: Visualization and Automatic Classification, ACM VizSec,2011