

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/338843538>

Interpreting Machine Learning Malware Detectors Which Leverage N-gram Analysis

Conference Paper · January 2020

CITATIONS

0

READS

177

2 authors:



William Briguglio

University of Windsor

7 PUBLICATIONS 4 CITATIONS

SEE PROFILE



Sherif Saad

University of Windsor

30 PUBLICATIONS 680 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



The Curious Case of Machine Learning In Malware Detection [View project](#)



Location Privacy in VANET [View project](#)

Interpreting Machine Learning Malware Detectors Which Leverage N-gram Analysis

William Briguglio and Sherif Saad

School Of Computer Science, University of Windsor, Canada
{briguglw,shsaad}@uwindsor.ca

Abstract. In cyberattack detection and prevention systems, cybersecurity analysts always prefer solutions that are as interpretable and understandable as rule-based or signature-based detection. This is because of the need to tune and optimize these solutions to mitigate and control the effect of false positives and false negatives. Interpreting machine learning models is a new and open challenge. However, it is expected that an interpretable machine learning solution will be domain specific. For instance, interpretable solutions for machine learning models in health-care are different than solutions in malware detection. This is because the models are complex, and most of them work as a black-box. Recently, the increased ability for malware authors to bypass antimalware systems has forced security specialists to look to machine learning for creating robust detection systems. If these systems are to be relied on in the industry, then, among other challenges, they must also explain their predictions. The objective of this paper is to evaluate the current state-of-the-art ML models interpretability techniques when applied to ML-based malware detectors. We demonstrate interpretability techniques in practice and evaluate the effectiveness of existing interpretability techniques in the malware analysis domain.

Keywords: Cybersecurity, Machine Learning, Malware Detection, N-Gram, Malware Detector Interpretability, Model Robustness, Model Reliability

1 Introduction

Adopting sophisticated machine learning techniques for malware detection or other cyber attack detection and prevention systems in a production environment is a challenge. This is because most of the time it is not possible to understand how machine learning systems make their detection decisions. In the malware detection domain, machine learning models can be trained to distinguish between benign binaries and malware, or between different malware families. The advantage of using machine learning models is that they are less sensitive to minute changes in malware binaries and can therefore detect unseen samples so long as they are designed and trained to detect characteristics common across seen and unseen samples. Furthermore, they're learnt relationships can be used

to determine relevant features for a classification, limiting the amount of data malware analyst must sift through to determine the functionality of a malicious binary. However, there are several drawbacks that must be addressed before their full potential can be realized in the malware detection domain. Firstly, due to the quick evolving nature of malware, the models must be made efficient to train and update frequently when new malware families are discovered. Secondly, it is possible to create specially crafted “adversarial samples” which take advantage of peculiarities in the models learnt relationships to bypass the detector with relatively inconsequential changes to the binary. Finally, given the high degree of risk involved with classification errors, the models must provide a reason for their decisions in order to improve performance and increase trust in the model and its predictions. This last point is the focus of this paper.

The process of providing reasons for a machine learning model’s predictions is known as interpretation. Interpretation in this setting should provide several key benefits. Firstly, due to the high cost of classification error, a low false positive and false negative rate is a must, and therefore these systems must be robust. A model is said to be robust if small changes in input do not cause large changes in output such as a different classification. Second, the high risk necessitates a high degree of model confidence. Therefore, interpretation must provide evidence that the model has learnt something which can be corroborated with industry knowledge. This also goes hand in hand with the first requirement as an interpretation which can show a model is robust can improve model confidence as well. Additionally, the interpretation should aid malware analysts in downstream tasks such as determining the functionality of a malware binary.

Machine learning interpretation can be broadly separated into two categories. One is model agnostic techniques which are independent of the type of model which they are interpreting and rely solely on the input and output of the model. The other, which we will be using in this paper, are model specific techniques, which use specific elements of the model such as learnt weights or decision rules in order to provide an interpretation of a prediction. Interpretations themselves can be divided into global and local interpretations. Global interpretations provide an interpretation that is applicable across the entire feature space. Meanwhile local interpretations apply to only a single example or a small subset of the feature space. Some interpretation techniques provide only one type of interpretation while others provide both.

In this paper we explore the interpretability of machine learning based malware classifiers in relation to the goals of model robustness, confidence in model predictions, and aiding the process of determining the functionality of a malware sample. We train a logistic regression model, random forest, and a neural network on a Microsoft data set containing the hexadecimal representations of malware binaries belonging to several different malware families. We then apply model specific interpretation techniques to provide both a global and local interpretation of each of the models. The objective of this paper is to demonstrate interpretability techniques in practice on machine learning based malware detectors. We also try to evaluate the effectiveness of existing interpretability

techniques in the malware analysis domain in terms of their usefulness to malware analysts in a practical setting. To the best of our knowledge, this is the only work which explores the application of machine learning interpretability techniques in the malware analysis domain.

2 Literature Review

In the last decade, with the increasingly massive data sets machine learning algorithms are being used on, and the growing complexity of the algorithms, the prediction process of these algorithms has become so non-intuitive that traditional analysis techniques no longer suffice. Analysis being necessary for a number of practical and legal concerns has caused research to now shift towards machine learning interpretability.

Christoph Molnar [11] put together a summary of machine learning interpretation methods in which he outlines a basic approach for the interpretation of Linear Regression models (of course the same approach can be applied to linear SVMs, Shirataki et al. [18]) where a features contribution to a prediction is the product of its value and weight. For logistic regression he shows that when the j^{th} feature value is incremented by 1, then the quotient of the predicted odds of the sample belonging to the positive class after the increase over the predicted odds of the sample belonging to the positive class before the increase is equal to e^{β_j} , where β_j is the weight of feature j . Alternatively, this means that a unit increase in feature j results in the predicted odds increasing by $((e^{\beta_j} - 1) * 100)\%$. He goes on to discuss the seemingly trivial interpretation of decision trees as the conjunction of the conditions described in the nodes along a predictions path to a leaf node. Similarly, for rule list models, an “explanation” is simply re-stating the rule or combination of rules which lead to a decision.

However, the evaluation of a models complexity is closely tied with its explanations comprehensibility, especially for rule set models, linear models, and tree models. Given the following complexity definitions, the explanation approaches discussed above could be too complex for highly dimensional datasets. Marco Ribeiro et al. [15] define the complexity of a linear model as the number of non-zero weights and the complexity of a decision tree as the depth of the tree. Meanwhile, Otero and Freitas [12] defined the complexity of a list of rules as the average number of conditions evaluated to classify a set of test data. They referred to this as the “prediction-explanation size”.

There has also been work done on the interpretability of neural networks(NNs) such as the Layer-wise Relevance Propagation introduced in [3] as a set of constraints. The constraints ensure that the total relevance is preserved from one layer to another as well as that the relevance of each node is equal to the sum of relevance contributions from its input nodes which in turn is equal to the sum of relevance contributions to its output nodes. Any decomposition function following these constraints is considered a type of Layer-wise Relevance Propagation. In [19], Shrikumar et al. propose DeepLIFT which attributes to each node a contribution to the difference in prediction from a reference prediction by back

propagating the difference in predication scaled by the difference in intermediate and initial inputs.

Moving on to model agnostic methods, Friedman in [6] used Partial Dependence Plots (PDP) to show the marginal effect a feature has in a predictive model. Similarly, Goldstein et al. [8] used Individual Conditional Expectation (ICE) plots to show a curve for each sample in the data set where one or two features are free variables while the rest of the features remain fixed. Since ICE plots and PDPs do not work well with strongly correlated features, Deniel W. Apley et al. [2] proposed Accumulated Local Effects plots to display the average local effect a feature has on predictions.

The H-statistic was used by Friedman and Popescu in [7] (equations 44-46) to provide a statistical estimate of the interaction strength between features by measuring the fraction of variance not captured by the effects of single variables. Feature Importance was measured by Breiman [4] as the increase in model error after a feature’s values are permuted (a.k.a. permutation importance).

Marco Ribeiro et al. in [15] defined a version of the surrogate method which can explain individual predictions using an approach called Local Interpretable Model-agnostic Explanations (LIME) which trains an interpretable classifier by heavily weighing samples nearer to a sample of interest. Tomi Peltola [13] extended this work with KL-LIME, which generated local interpretable probabilistic models for Bayesian predictive models (although the method can also be applied to non-Bayesian probabilistic models) by minimizing the Kullback-Leibler divergence of the predictive model and the interpretable model. This has the added benefit of providing explanations that account for model uncertainty. Strumbelj et al. [20] detailed how to describe the contributions made by each feature to a prediction for a specific instance using Shapely Values, a concept adopted from coalitional game theory.

Finally, there are Example-Based methods such as the method put forward by Wachter et al. in [21] which produce interpretations by finding counter-factual examples which are samples with a significant difference in prediction, whose features are relatively similar to the sample of interest, by minimizing a loss function. The found sample is then used to explain what small changes would cause the original prediction to change meaningfully. There is also the MMD-critic algorithm by Kim et al. [9] which finds Prototypes (well represented examples) and Criticisms (poorly represented examples) in the dataset. To find examples in the training data which have a strong effect on a trained linear regression model (i.e. influential instances) Cook [5] proposed Cook’s distance, a measure of the difference in predictions made by a linear regression model (however the measure can be generalized to any model) trained with and without an instance of interest. Koh and Liang [10] put forward a method for estimating the influence of a specific instance without retraining the model as long as the model has a twice differentiable loss function.

3 Method

Training and classification were done on a data set of 10,896 malware files belonging to 9 different malware families.¹ The data set is discussed in [16]. Each sample consists of the hexadecimal representation of the malware’s binary content. The class details are summed up in table 1.

Table 1. Class distribution in Data Set

Class No.	Family	Sample Count	Type
1	Ramnit	1541	Worm
2	Lollipop	2478	Adware
3	Kelihos_ver3	2942	Backdoor
4	Vundo	475	Trojan
5	Simda	42	Backdoor
6	Tracur	751	TrojanDownloader
7	Kelihos_ver1	398	Backdoor
8	Obfuscator.ACY	1228	obfuscated malware
9	Gatak	1013	Backdoor

Based on other work on the the same data set, we decided to use n-grams as features. N-grams are sequences of words of length n which occur in a body of text. However, in our case the n-grams are sequences of bytes of length n which occur in a binary. The length of n-gram we settled on was 6 because they were shown to preform well in [14], however our approach can work with n-grams of arbitrary length. We extracted the 6-gram features from the hex representations of the malware files by obtaining the entire list of 6-grams present in the data set, and the number of files each 6-gram appeared in. This resulted in over 2,536,629,413 candidate features. Next, any 6-gram which did not appear in at least 100 files was removed from consideration, bringing the feature set size down to 817,785. This was done because [14] also showed that selection by frequency is an effective way to reduce the initial feature set size and a computationally cheap approach was needed considering the number of features.

Next, feature vectors were created for each of the malware samples so that a more sophisticated feature selection method can be preformed. This was done by searching for the selected 6-gram feature in a binary and setting the corresponding value in that binary’s feature vector to 1 if the binary did contain the 6-gram, and 0 otherwise. To select the features for the logistic regression model, Chi^2 was used because it can detect if a categorical feature is independent of a predicted categorical variable (in this case our class) and is therefore irrelevant to our classifier. For the neural network and random forest, Mutual Information (MI) was used because it can detect the more complex dependencies between a

¹ The data set was downloaded from <https://www.kaggle.com/c/malware-classification/data>

feature and a sample’s classification which can be taken advantage of by a neural network or random forest. Since the feature set was still very large, the Chi^2 and MI scores had to be calculated in batches. This was done by splitting the data set into 20 batches, each with the same distribution of classes, and averaging out the resulting scores for each feature. Next, the features with Chi^2 scores above 330 or MI scores above 0.415 were selected. This brought the feature set size down to 8867 in the case of the logistic regression model and to 9980 in the case of the neural network and random forest. The feature set size was determined based off other work using n-grams to classify the same data set. We did not attempt to find an optimal feature set size as our primary focus was model interpretation.

Next, the models were trained on their respective feature sets. To find the best parameters for the logistic regression model and train the model, grid search with 5-fold cross validation was used, yielding $C = 10$ and $\text{tolerance} = 0.0001$. The value of C inversely determines the strength of regularization, that is, smaller values of C cause more feature weights in the classifier to be set to 0, a value of 0 corresponds to no regularization, and values above 0 encourage the classifier to use more features. Tolerance determines the minimum change in error, from one iteration of the optimization algorithm to the next, that causes the algorithm to terminate training. Similarly for random forest, finding the best parameters and training was done with grid search with 5-fold cross validation as well. The number of trees found to perform best was 300 and the minimum samples per leaf found to perform best was 0.01% of the total number of samples. The grid search with cross validation, logistic regression model, and the random forest model were implemented using the scikit python library.

For the neural network the data was split into a training and a test set each with the same class distribution. This was done because the extra parameters in a neural network require a larger data set to learn more abstract patterns and splitting it up into many folds might have stifled this process. The neural network consisted of an input layer with one neuron per feature, an output layer with one neuron per class using the sigmoid activation function, and a hidden layer consisting of 40 neurons using the tanh activation function. 40 neurons was chosen because that number was found to perform the best after testing with various other configurations. There were also no bias units to aid in interpretation. The neural network was implemented using the Keras python library.

After training and testing the three models, the logistic regression model was interpreted by examining the weights used by the classifier. The random forest was interpreted by examining the feature importance as well as using the `treeInterpreter` python library [17] to obtain feature contributions to a particular prediction. In the case of the Neural network, the `iNNvestigate` python library by [1] was used to perform LRP to get the relevances of each node in the model for interpretation. The balanced accuracy on the left out fold was 96.19% for the logistic regression model and 96.97% for the random forest. The balanced accuracy on the test set was 94.22% for the neural network. A discussion of the model interpretations follows in the next section.

4 Interpretation

Logistic Regression Model Interpretation The logistic regression model uses a one-vs-rest classification scheme whereby for each class, a constituent model is trained to classify a sample as either that class, or not that class, and therefore we are actually dealing with nine separate logistic regression models each making binary classifications. For this reason we cannot perform the typical global interpretation of the overall multi-class model by examining the weights since the weights should be different for each of the binary models. However, we can gain insight of the importance of each feature by averaging these weights across the 9 constituent binary models. For this we take the average of the absolute values of the weights. This is because if a feature contributes positively for one constituent binary classifier and negatively for another, then the weights would cancel each other out during averaging which would falsely give the impression that the feature was not important in the overall multi-class model. Table 2 shows the largest 15 averages of the absolute feature weights.

Table 2. Max 15 Absolute Weights of the Logistic Regression Model Averaged Across All 9 Binary Sub-classifiers

Avg. Abs. Weight	Feature
1.3151053659364556	0000000066C7
1.3480135328294032	008B4C240C89
1.4629237676020752	8BEC83EC10C7
1.4846778818947817	00000000EB07
1.5276044995023308	B80000000050
1.540535475655897	500147657453
1.5605614219830626	006800004000
1.6494330450079937	89852CFDFFFF
1.685741868293823	0033C58945FC
1.7235671007282005	8B91C8000000
1.781357432072784	034C6F61644C
1.8232074423648363	8BEC6A006A00
2.071327588344743	00E404000000
2.15007904223129	0083C4088B4D
2.1561672884172056	C78530FDFFFF

Looking at the table 2, we can see that three 6-grams are relatively heavily weighted, 00E404000000, 0083C4088B4D, and C78530FDFFFF. Recall from section 2 that for logistic regression, when the j^{th} feature value is incremented by a value of 1, then the predicted odds increase by $((e^{\beta_j} - 1) * 100)\%$, where β_j is the learnt weight of the j^{th} feature. In our case we are using binary feature values where a 1 indicates the presence of a 6-gram and 0 indicates its absence, so we interpret the weights as follows. When the 6-gram corresponding to the j^{th} feature is present, the predicted odds increase by $((e^{\beta_j} - 1) * 100)\%$.

One may be tempted to apply this to the weights in table 2, but these are averaged *absolute* weights across all 9 constituent binary classifiers. Further, negative weights do not cause a decrease in the predicted odds that is proportional to a positive weight with the same absolute value due to the shape of the function $f(x) = e^x - 1$. Therefore, it would be inaccurate to say the average absolute effect of some 6-gram corresponds to a $(e^{avg_j} - 1)\%$ change in the predicted odds, where avg_j is the average absolute weight of feature j . Thus a global interpretation of a multi-class one-vs-rest logistic regression model using n-grams is confined to vague statements about which n-grams are important based solely off their average absolute weights, which is not very useful in a practical setting.

Next we will examine the max weights for a constituent binary model. This will allow us to make conclusions on what features the model uses to detect a specific class of malware in the data set. Furthermore, we will be able to determine exactly the change in predicted odds that the presence of an n-gram causes. For the sake of brevity, we will examine just the binary model for class 3, corresponding to the Kelihos_ver3 family of malware, as all three models performed well for this class but the same process can be followed for the other constituent binary models corresponding to other classes. Table 3 shows the max 15 weights of the classifier for class 3.

Table 3. Max 15 Weights for Kelihos_ver3 Binary Sub-classifier

Weight	Feature
0.6438606978376447	000607476574
0.6438606978376447	000C07476574
0.6438606978376447	060747657444
0.6438606978376447	074765744443
0.6438606978376447	0C0747657444
0.6438606978376447	930644697370
1.3719246726968015	00000083FEFF
1.5114878196031336	E8000000895D
2.1067800174989904	0F85CC010000
2.3123117293223405	0A0100008B45
2.9041700918303084	000F859D0000
3.174276823535364	000F84700100
3.5334477027408613	0083C4088B4D
3.7941081330633857	034C6F61644C
4.391600387291376	00008B5DE43B

In table 3 we can see three 6-grams have relatively large weights. This means these n-grams are most strongly associated with class 3 and in this case, since we are looking at only the weights for a single binary classifier, we can use our interpretation from above. That is, when the 6-gram corresponding to the j^{th} feature is present, the predicted odds increase by $((e^{\beta_j} - 1) * 100)\%$. For

example we can say the presence of 00008B5DE43B, increases the predicted odds of a sample belonging to class 3 by $((e^{4.3916} - 1) * 100)\% = 7977\%$. At first glance this number may seem excessive but in order to make good sense of it we must also determine what the predicted odds of a sample belonging to class 3 are when this 6-grams are not present, using a reference sample. For this we use a zero-vector corresponding to a sample where none of the 6-grams used as features are present. Since the dot product of a zero vector and the weight vector is zero, we only need to take the sigmoid of the intercept of the binary model for class 3 to determine the predicted probability of the reference vector belonging to class 3. The intercept is -4.2843, thus the predicted probability of the reference sample belonging to class 3 is $\text{sigmoid}(-4.28426) = 0.01360$. Next we must convert this to odds with $0.01360/(1 - 0.01360) = 0.01378$. This means a sample with no feature 6-grams present except 00008B5DE43B increases the odds from 0.01378 by 7977% to $0.01378 + (0.01378 * 79.77) = 1.11301$ predicted odds, or a 0.5267 predicted probability, of belonging to class 3. Thus we see that because of the intercept, the large weight of this feature does not necessarily guarantee a classification into class 3.

We can get a better idea of the robustness of the model by checking the number of 6-grams which play a significant role in the classification of a sample into class 3. This is because robustness is a measure of how tolerant a model is to small changes in input. Therefore, if the number of 6-grams which play a significant role is large, then a large number of changes in input will be required for a change in classification, thus giving us confidence in the model's robustness. However, if the number of significant features is low then only a small number of changes in input will be required for a change in classification, changes that may be easy and inconsequential for malware authors to make. Thus the robustness of the model would be called into question. In our case, 20 features have weights greater than or equal to about 0.59. 6-grams with weights above this number increase the predicted odds by $((e^{0.59} - 1) * 100)\% \approx 80\%$. Since the predicted odds of the reference example belonging to class 3 is 0.01378, this means about 11 such features can cause a sample to be classified as class 3 with about 90% predicted probability. This may indicate that the model is putting too much emphasis on just a few highly weighted 6-grams. To test this we can reclassify samples belong to class 3 with the highest weighted 6-grams set to 0. In our case, we set the nine highest weighted features to 0 for all samples. This required 22863 changes to the feature array, and the result was only 24 more misclassifications, 17 of which belonged to class 3, which has 2942 samples. Here, we encounter a specification issue. Currently, there is no formally defined metric to measure robustness quantitatively and once there is, a threshold for acceptable robustness will be application specific. We leave a definition of a robustness metric to future work, however, given that robustness is defined in terms of a model's tolerance to changes in input, and that tolerance to changes of insignificant features is irrelevant, we can be confident that this approach can give us an idea of our model's robustness. The models robustness becomes more clear when compared with other models. For example, if setting the same number of

features to 0 in another model resulted in more or less misclassification, then we can say that model is less or more robust respectively than our logistic regression model. Therefore, we can confidently say our approach gave an idea of model robustness for class 3. One can increase the model’s robustness by further training the classifier with samples which have the highly weighted 6-grams removed. This would force the classifier to learn a more diverse set of features which correspond to class 3, meaning that more changes would be required to change a prediction to or from class 3. Thus by observing the important features, we can improve the models robustness to small changes in the input. A similar strategy can be followed for the most negatively weighted features. If there are features with too large negative weights, then a detector can be fooled by intentionally adding these 6-grams. Further training the classifier by adding the large negative weighted 6-grams to samples labeled class 3 will force the classifier to learn not to negate positively weighted features with one or a small set of 6-grams. Therefore we can conclude that examining the weights in the manner we have done here can be useful for debugging logistic regression models leveraging n-grams. This interpretation is still global in that it encompasses the entire feature space, however, it must be repeated for each class. On the upside though, the global interpretation doubles as a local interpretation as the relationship between the presence of an n-gram and the change in the predicted odds holds across the entire data set for each sample.

Furthermore, this method for finding important n-grams features can be helpful in a practical setting as it can be used to aid malware analysts in downstream tasks. A malware binary’s functionality can be more easily determined by implementing a method which automatically disassembles binaries and highlights the code which corresponds to the most heavily weighted n-grams that are present in the binary. This approach can also improve confidence in the model if the highlighted code’s functionality is corroborated with industry knowledge. Both these advantages require another interpretation step of mapping feature values from the feature space to the domain space (i.e. mapping n-grams to the corresponding code) which is not the focus of this paper. The downside to this interpretation approach is that it is specific to logistic regression models only, and unlike models such as neural networks or decisions trees, logistic regression models are not easily capable of learning more complex relationships between features and target values.

Random Forest Interpretation In the case of the random forest, interpretation is more difficult. It is easy in a more general sense, in that we can get the feature importance scores, shown below in table 4, and use these to determine what features are generally most important, but getting a more fine grained interpretation is a challenge as the random forest is an ensemble of often hundreds of different decision trees.

Table 4 gives us a great idea of the model robustness. Since the total feature importance is always equal to 1, we can be sure that the model isn’t relying on just a small number of features to make predictions because the 15 most important features only accounts for 0.9% of the total importance. Additionally,

Table 4. Max Feature 15 Importances for Random Forest

Feature Importance	Feature
0.006877917709695	726573730000
0.007047751117095	7450726F6341
0.00723117607771	647265737300
0.007262894349522	558BEC83EC08
0.007377076296786	0064A1000000
0.007401045194749	727475616C41
0.007815881804511	A10000000050
0.008221953575956	75616C416C6C
0.008652467124996	634164647265
0.008657476622364	8A040388840D
0.008840768087294	69727475616C
0.008879491127129	89F5034C2404
0.00898170788833	7475616C416C
0.008987620418762	008A840D2F06
0.009011931204589	060000E2EFB9

the feature importance steadily declines without one feature or a small group of features overshadowing the rest. Unfortunately, general statements about robustness which do not provide much utility to the malware analyst in a practical setting are the most we can say with a global interpretation. However considering a single example can give us more information, albeit only locally.

Interpretation of a Single Sample with Random Forest With random forest, a local interpretation of a single example is difficult as a classification decision is the result of a vote amongst many different decision trees. However, here we find the tree with the highest predicted probability that a specific example belongs to its actual class. Then we use the tree interpreter library [17] to break down the contributions of each 6-gram feature. In our case we followed this procedure for sample 4WM7aZDLCmlosUBiqKOx and found that the 6-gram 002500000031 and the bias contributed 97.3% of the total feature importance. One may be tempted to think this means the model is relying on only a single feature however this is just one tree out of many which have heavily varying structures. Thus, changing this feature may not cause many of the other tree’s predictions to change, such is the advantage of using random forests over single decisions trees. The significance of the resulting feature contribution is two fold. Firstly, the model designer can find the code corresponding to 002500000031 in the assembly code and determine weather the functionality of the code corroborates industry knowledge. If it does, then this can be used with other examples to improve model confidence. Secondly, by finding 6-grams in the constituent decision trees of the random forest model which are significant to a prediction, a process can be automated to disassemble the input file and highlight the code that corresponds to these significant 6-grams, aiding in malware analysis. The downside to this approach is that the random forest is made up of many differ-

ent decision trees, many of which should all be predicting the correct class, so an automated process which collects significant 6-grams from these constituent trees and highlights the corresponding code may provide an overwhelming number of results. This is because well over a hundred trees will be contributing at least a few 6-grams, meaning that potentially 100's of snippets of code will be highlighted to the analyst. Once again we are faced with the problem of mapping the feature values to the domain, however this should not be too tall a task and we leave this challenge to future work.

Neural Network Model Interpretation For our global interpretation of the Neural Network model, we used LRP to determine the most relevant input nodes for classification. LRP was preformed in this experiment using iNNvestigate python library by [1]. First we found the relevances of the input nodes for each sample and then we averaged the absolute values of these relevances for the entire data set. This was done because one input node may be positively contributing to one output nodes prediction while negatively contributing to another, causing the input nodes relevances to cancel out during averaging and giving false impressions about the feature set. Table 5 shows the largest 15 averages of the absolute relevances.

Table 5. Max Average Absolute Relevances

Avg. Abs. Relevance	Feature
0.4204155570273673	24000000008B
0.438576163384531	75616C416C6C
0.4604056179848827	000400000000
0.6358686047042836	00FFFFFFFFFF
0.6414918343055965	008A840D2F06
0.6961477693970937	060000E2EFB9
0.7207968499760279	8A040388840D
0.7391062783969391	000001000000
0.7655264716760353	040000000000
0.7695977668414099	89F5034C2404
0.8623695409436033	416C6C6F6300
0.8762457266039623	6C6C6F630000
0.8811945910382549	69727475616C
1.1011308772023591	000000000400
1.129173981900078	0000000000FF

Bolded 6-grams also present in Table 4

Table 6. Max Avg Relevances for Class 3

Avg Relevance	Feature
0.07849652902147494	060747657444
0.0858714786617495	8B0000006700
0.08840799934653523	07497357696E
0.09155762345728868	0C0747657444
0.09213969967088875	F10448656170
0.09360746295067239	00F0F0280000
0.09471450612061977	00F104486561
0.10572475395119978	C3008BFF558B
0.10603324133390207	009306446973
0.11341626335133194	000C07476574
0.11451772113662628	C38BFF558BEC
0.12097247805393918	930644697370
0.14448647700726405	04546C734765
0.1895982317973578	064469737061
0.24520372442763907	034C6F61644C

Bolded 6-grams also present in Table 3

In Table 5 we can see two values had significantly higher relevances than the rest, 000000000400 and 0000000000FF, and are therefore important for the models classification. Additionally, we can see many of the features which appear here are also in the top 15 most important 6-grams for the random forest. This

result partially validates our technique for finding important 6-gram features in a neural network which to the best of our knowledge is a novel use of LRP in this domain. This gives us a general idea of the importance of features used by the model but, just like in the case of the other two models, we are still confined to vague general statements about a feature’s importance. However, this time it is due to the complexity of the model.

Next we will examine the max relevances for a particular class. In this case we average the relevances for each node across all samples which were correctly classified as class 3. Table 6 shows the max 15 average relevances for class 3.

In Table 6 we can see five of the features which appear here are also in the top 15 highest weighted 6-grams for the binary logistic regression classifier for class 3. This result also partially validates our technique for finding important 6-gram features in a neural network for a single class. In this case we are still confined to general statements about a features importance for a specific class. However, we can get an idea of the model’s robustness by setting the features with the highest average relevances for class 3 to 0 for all correctly classified samples in class 3. If the model relies heavily on only the presence of these 6-grams, then the class accuracy will drop drastically, however if we have a similar class accuracy as before, then it is unlikely that the features with a lesser average relevance would have a larger effect on the class accuracy and therefore we can somewhat confidently say the model is robust for this class. In our experiment the top 4 highest average relevance features were all set to 0 and it resulted in no further misclassifications. Therefore we can say our model is somewhat robust for class 3. This result is somewhat helpful in a practical setting as a malware analyst can use this technique to ensure the robustness of their model, but not much else.

Interpretation of a Single Sample with Neural Network

Next we’ll further explore the neural network’s predictions for samples belonging to class 3 by taking the test sample with the highest predicted probability of belonging to class 3, sample 4WM7aZDLCmlosUBiqKOx, and examining relevances for this sample in order to provide a local interpretation. In doing so we can see what the internal nodes are learning. First we determine the internal node relevances for this sample. The library used for this experiment did not have a built in method to determine the relevances of internal layer nodes so we created a second neural network that was a duplicate of the last two layers of the original neural network. We then obtained the value of the second layer nodes before the activation function is applied when classifying this sample. That is, if W^1 is the weight matrix for the connections between layer 1 and layer 2, and X^1 is the outputs of layer 1, then we obtained $X^1 \cdot W^1$. We then inputted $X^1 \cdot W^1$ into our second neural network and performed LRP to get the relevances of the first layer of our second neural network which are equivalent to the relevances of the hidden layer in our original neural network. The most relevant node by a substantial margin was the 40th node in the hidden layer with a relevance of 0.61 and an activation of -0.99996614. Since this node is in layer 2 we will denote it with n_{40}^2 . Next we created a third neural network that had two layers. The

first was identical to layer 1 of our original neural network, the second was just the single node, n_{40}^2 , from the original neural network, and the weight matrix for the connections from layer 1 to layer 2 of this new network is $W_{(40)}^1$ where $W_{(i)}^1$ is the 9980-dimensional weight vector for connections from layer 1 to the i^{th} node in layer 2 of the original neural network. In this way we were able to obtain the relevances of the input layer to only the activation of n_{40}^2 in the hidden layer. Table 6 shows the max 10 node relevances for the activation of n_{40}^2 in the hidden layer.

Table 7. Layer 1 Nodes relevance to n_{40}^2

Activation	Relevance	Feature
1.0	0.025721772	007300000061
1.0	0.027428055	230000001900
1.0	0.02751717	2F0000002300
1.0	0.029254071	270000003300
1.0	0.030343212	00870000009D
1.0	0.03163522	002F00000025
1.0	0.031697582	040000C00000
1.0	0.03176714	002300000019
1.0	0.032007236	00C0000000D0
1.0	0.034308888	007701476574

In table 7 we can see that many of the 6-grams have similar relevance's which slowly decrease. This corroborates our results when examining class 3 as a whole since the similar relevances across many input nodes indicates that many features are responsible for a classification which is to be expected when a model is robust to changes in the input data. One can automate the process of performing LRP on specific examples to find relevant input nodes, both for the entire model and for a specific internal node possibly showing what the internal node is learning. From there highlighting the disassembled code which corresponds to the most relevant nodes can help malware analyst either determine the functionality of the file or show that the model has learnt something which corresponds to industry knowledge, thus improving confidence in the model.

5 Conclusion

In this paper we demonstrated techniques for the interpretation of malware detectors which leverage n-grams as features. We've shown that it is possible to interpret a neural network, a logistic regression model, and a random forest, with the objectives of debugging and creating robust models, improving model confidence, and aiding malware analysts in downstream tasks. For the logistic regression model, examining the weights was all that was needed to meet

these goals. However, although straight forward to interpret, the model was less expressive than the other two considered. The random forest required slightly more work for analysis but it was also possible to get a meaningful local interpretation that helped with the above stated goals. The downside here was that the random forest interpretation must consider many of constituent trees to be thorough, which can be time consuming and result in too much data. The neural network interpretation was much more intensive but by using layer-wise relevance propagation it was possible to determine the relevance or significance of different n-grams across the data set, across a specific class, and for a single example or for a single node. Thus, we were able to provide a global and local interpretation which was somewhat useful in a practical setting since by using these relevances it was then possible to get an idea of the robustness of the model and build confidence or aid in downstream analysis of samples.

Over all it was possible to satisfy our interpretation objectives for each model but the ubiquitous trade off between the interpretability and the expressivity of the model was still present. Additionally, n-grams in and of themselves seem slightly problematic as it is not easy to determine what a n-gram corresponds to on its own, without considering a single example for context. So providing a global interpretation of a n-gram in order to show what the model has learnt is difficult. To this end it would be advantageous to include human readable features as well or other features which can be easily interpreted in a manner that doesn't require examining a real specific example. For future work we will focus on evaluating model agnostic techniques and enabling explanations in specific domain applications such as malware detection.

References

1. Alber, M., Lapuschkin, S., Seegerer, P., Hgele, M., Schtt, K.T., Montavon, G., Samek, W., Mller, K.R., Dhne, S., Kindermans, P.J.: innvestigate neural networks! (2018)
2. Apley, D.W., Zhu, J.: Visualizing the effects of predictor variables in black box supervised learning models (2016)
3. Bach, S., Binder, A., Montavon, G., Klauschen, F., Müller, K.R., Samek, W., Suárez, O.D.: On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. In: PloS one (2015)
4. Breiman, L.: Random forests. *Machine Learning* **45**(1), 5–32 (Oct 2001). <https://doi.org/10.1023/A:1010933404324>, <https://doi.org/10.1023/A:1010933404324>
5. Cook, R.D.: Detection of influential observation in linear regression. *Technometrics* **19**(1), 15–18 (1977). <https://doi.org/10.1080/00401706.1977.10489493>, <https://doi.org/10.1080/00401706.1977.10489493>
6. Friedman, J.H.: Greedy function approximation: A gradient boosting machine. *Ann. Statist.* **29**(5), 1189–1232 (10 2001). <https://doi.org/10.1214/aos/1013203451>, <https://doi.org/10.1214/aos/1013203451>
7. Friedman, J.H., Popescu, B.E.: Predictive learning via rule ensembles. *Ann. Appl. Stat.* **2**(3), 916–954 (09 2008). <https://doi.org/10.1214/07-AOAS148>, <https://doi.org/10.1214/07-AOAS148>

8. Goldstein, A., Kapelner, A., Bleich, J., Pitkin, E.: Peeking inside the black box: Visualizing statistical learning with plots of individual conditional expectation. *Journal of Computational and Graphical Statistics* **24** (09 2013). <https://doi.org/10.1080/10618600.2014.907095>
9. Kim, B., Khanna, R., Koyejo, O.: Examples are not enough, learn to criticize! criticism for interpretability. In: *Proceedings of the 30th International Conference on Neural Information Processing Systems*. pp. 2288–2296. NIPS’16, Curran Associates Inc., USA (2016), <http://dl.acm.org/citation.cfm?id=3157096.3157352>
10. Koh, P.W., Liang, P.: Understanding black-box predictions via influence functions. In: *Proceedings of the 34th International Conference on Machine Learning - Volume 70*. pp. 1885–1894. ICML’17, JMLR.org (2017), <http://dl.acm.org/citation.cfm?id=3305381.3305576>
11. Molnar, C.: *Interpretable Machine Learning*. GitHub (2019), <https://christophm.github.io/interpretable-ml-book/>
12. Otero, F.E., Freitas, A.A.: Improving the interpretability of classification rules discovered by an ant colony algorithm. In: *Proceedings of the 15th Annual Conference on Genetic and Evolutionary Computation*. pp. 73–80. GECCO ’13, ACM, New York, NY, USA (2013). <https://doi.org/10.1145/2463372.2463382>, <http://doi.acm.org/10.1145/2463372.2463382>
13. Peltola, T.: Local interpretable model-agnostic explanations of bayesian predictive models via kullback-leibler projections. *ArXiv* **abs/1810.02678** (2018)
14. Raff, E., Zak, R., Cox, R.J., Sylvester, J., Yacci, P., Ward, R., Tracy, A., McLean, M., Nicholas, C.: An investigation of byte n-gram features for malware classification. *Journal of Computer Virology and Hacking Techniques* **14**, 1–20 (2016)
15. Ribeiro, M.T., Singh, S., Guestrin, C.: ”why should i trust you?”: Explaining the predictions of any classifier. In: *Proceedings of the 22Nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. pp. 1135–1144. KDD ’16, ACM, New York, NY, USA (2016). <https://doi.org/10.1145/2939672.2939778>, <http://doi.acm.org/10.1145/2939672.2939778>
16. Ronen, R., Radu, M., Feuerstein, C., Yom-Tov, E., Ahmadi, M.: Microsoft malware classification challenge (2018)
17. Saabas, A.: *Treeinterpreter*. <https://github.com/andosa/treeinterpreter> (2015)
18. Shirataki, S., Yamaguchi, S.: A study on interpretability of decision of machine learning. In: *2017 IEEE International Conference on Big Data (Big Data)*. pp. 4830–4831 (Dec 2017). <https://doi.org/10.1109/BigData.2017.8258557>
19. Shrikumar, A., Greenside, P., Kundaje, A.: Learning important features through propagating activation differences. *ArXiv* **abs/1704.02685** (2017)
20. Strumbelj, E., Kononenko, I.: An efficient explanation of individual classifications using game theory. *J. Mach. Learn. Res.* **11**, 1–18 (Mar 2010), <http://dl.acm.org/citation.cfm?id=1756006.1756007>
21. Wachter, S., Mittelstadt, B.D., Russell, C.: Counterfactual explanations without opening the black box: Automated decisions and the gdpr. *ArXiv* **abs/1711.00399** (2017)