Part 2: Machine Learning

Patrick Collins
1900609

Table of Contents

Abbreviations

RF: Random Forest

NB: Naïve Bytes

Context

ScottishGlen is a small company within the energy sector whose employees have been receiving messages from a hacktivist group, who threaten to target the company following a recent blog post by the CEO. It's unclear the nature of the attack they are planning. The CEO is concerned and has asked the IT manager to improve the security posture to better protect the company.

The focus is on making the company resilient to attack therefore the IT manager has asked the technical staff to assess (evaluate) the company's resilience to attack from obfuscated malware. The technical staff managed to get something up and running and have some data for analysis. The system memory appears to be prone to Spyware, Ransomware and Trojan malware but the team is not quite sure how to make sense of it.

Using Machine Learning Algorithms to Categorise Data

The sample data collected by the technical staff for Scottish Glen has multiple attack categories (See Appendices A&B). They are:

- Benign (meaning not malware)
- Spyware
- Ransomware
- Trojan

The technical staff has used a train-test split to get the data therefore it is suitable to choose a supervised learning approach to this problem as a training data set has been created to train the models to predict and classify each memory dump file.

Furthermore, as the objective is to categorise the data according to the attack category a suitable machine learning algorithm to choose would be a multi-class classification algorithm. For example, whether a system memory dump file is Ransomware, a Trojan, Spyware or Benign. This is due to the categories having more than two which a binary classification would be more suitable.

This would also be a form of document classification, sorting the memory dump files to the corresponding category. By doing so, it allows for making sense of the system memory more clearly and faster.

Random Forest

What is this algorithm?

A very popular multi-class classification algorithm is Random Forest. It is a supervised learning algorithm that enables classification of tasks using multiple decision trees. Random Forests can be used for both classification and regression. Classification is predicting the probability of a given class (category). Whereas regression is predicting continuous outcomes. Although, Random Forest is primarily helpful for classification problems.

How it does this is by selecting random samples from the given training set for growing the tree. Then it constructs decision trees for the chosen data points from this training data. The best split out of the variables is used to split the node.

Finally, the leaf node in each decision tree is the binary result that the tree ‘votes’ which is the most likely class. The most voted prediction result out of all choices is outputted as the final prediction result. It outputs either yes or no, true, or false, or in this case Ransomware or not, Spyware or Not, Trojan or not, Benign or not. The final binary output will be what the memory dump file is categorised as.

Figure 1 on the next page is an example diagram that the Random Forest would look like. Multiple decision trees are utilised, and the highlighted nodes show the decision making the algorithm is making outputting the result. The result from each decision tree is then used to produce the final binary result of the input data assigning the most probable class to it.

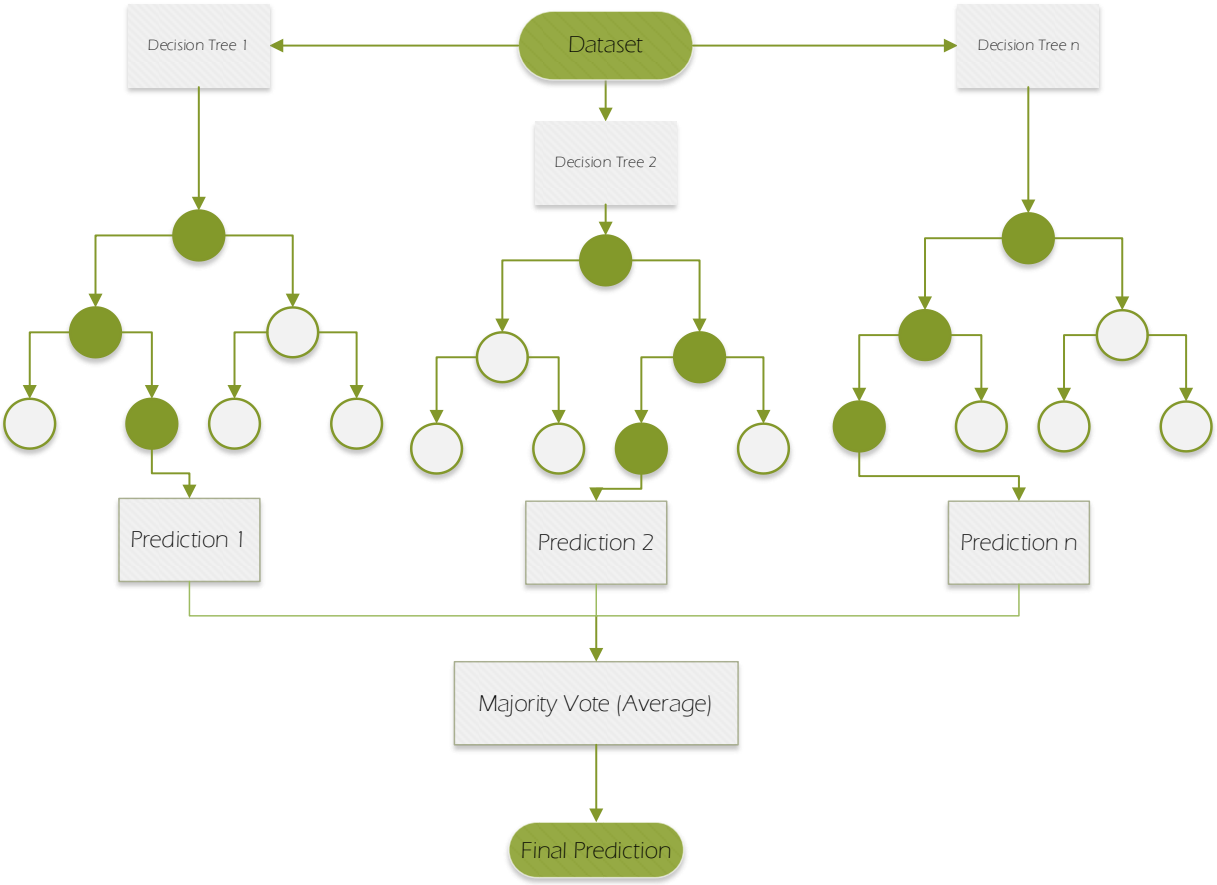

Figure 1: Random Forest

Strengths of RF

There are many strengths to choosing this algorithm to solve a problem. Random Forest fixes the overfitting problem present in standalone decision trees by using multiple trees and producing a result based on a majority vote or average.

Another benefit of choosing RF is that it is the best high-performance algorithm as it can run efficiently on very large datasets. The algorithm also provides flexibility as it can handle both regression and classification tasks making it popular choice for data scientists (IBM, 2023).

Weaknesses of RF

The downside to Random Forest is that it requires more resources as it processes a large dataset. Given this it then causes a time-consuming process as more time is required to process data for each individual decision tree in large data sets.

By providing the strength of more accurate predictions it needs more decision trees to do so, resulting in a slower model. This version of the bagging method is more complex as prediction of a single decision tree is easier to interpret than a random forest (IBM, 2023).

Limitations of RF

Random forest cannot be run when the data is very sparse as it will not produce good results. Some other algorithms like XGBoost perform better in these cases handling smaller data. Finally, if you need extrapolation of data random forest regression is not the best fit to solve this problem.

Naïve Bayes

What is this algorithm?

Another very popular multi-class classification algorithm is Naïve Bayes (NB) which is a supervised learning algorithm. This algorithm can be used for classification tasks, such as document classification making it suitable for categorising the files according to attack category.

The NB classifiers work differently in that they operate under a couple of key assumptions which is how it was given the name “Naïve” (IBM, 2023). It simplifies a classification problem by making it solvable in a smaller number of steps. Meaning that only a single probability is used for each variable making model computation easier (IBM, 2023). This algorithm works better with smaller data sets.

Class-conditional probabilities is the likelihood that a word is in a file. In an example where the file contains ransomware text the following formulae could be used to categorise it to appropriate class where y is ransomware (the class variable) and x is ransomware (feature) (IBM, 2023, Vadapalli, 2022):

$$P(y=[\ ransomware] \mid x=ransomware) = P(ransomware \mid\ ransomware)$$

Strengths of NB

Naïve Bayes is considered a simpler classifier since the parameters are easier to estimate (IBM, 2023). This makes it easy to understand and implement. The algorithm is considered a fast and efficient classifier that is fairly accurate unlike other models such as linear regression.

A benefit over Random Forest is this algorithm has low storage requirements as not a lot of resources is needed to process the data set. Depending on the classification problem to solve, like document classification, it can effectively manage a high number of dimensions (IBM, 2023).

Weaknesses of NB

However there are also some downsides to using this algorithm. One major one being it has zero frequency issues. If a category variable does not exist within the training set this will then cause an issue in the model (IBM, 2023). This could cause major problems therefore should only be chosen if the classification problem will be suitable for this. Another weakness is that the NB incorrect assumption can lead to incorrect classifications (IBM, 2023).

Limitations of NB

Finally, one limitation of Naïve Bayes is that it is not suitable for real world cases (Vadapalli, 2022). The algorithm is prone to assumptions that all features are independent which rarely happens in real world cases and should not be chosen for real-world applicability and classification problem solving.

Designing The Classifier

The IT manager recommends that ScottishGlen implement the Random Forest machine learning algorithm to make sense of the memory dump files. For the problem facing the business using a Random Forest is more suitable over Naïve Bayes as it will outperform it and run more efficiently.

A good rule of thumb to create a classifier is to complete all stages of a Data Pipeline. The technical team have already captured the data needed to create a classifier completing the Data Acquisition stage and then splitting it into training data and testing data (Appendix A & B).

Therefore, the first step the technical team should take is to perform data pre-processing on the training data. This is to reduce any variables that could disrupt the model process. The training set should be used for training the model and building the classifier which is the next stage of the pipeline.

To build the Random Forest classifier the team should focus on document classification. The goal of document classification is to create a classification model that can accurately assign documents to the right categories (Orza, 2022). As a reminder the categories are:

- Benign
- Spyware
- Ransomware
- Trojan

The classes in the forest should be set according to the attack category. The training data will first be fed to train multiple decision trees. Bootstrapping will then be performed with the algorithm selecting random samples. The algorithm will then construct a decision tree for every training data sample. As mentioned previously, the final prediction of all the decision trees will be the most likely category for each file.

Many programs may be utilised to complete this task though the IT manager recommends the team to use Python as the programming language and to use the “sklearn” python modules from Scikit-Learn. Its “RandomForestClassifier” is trained using bootstrap aggression making it very suitable for designing this classifier and for easy implementation (scikit, 2023).

Once the classifier model is ready the final stages which are to evaluate and test its accuracy using the testing data set which is discussed in the next section.

Evaluating Classifier Performance

The objective for this stage is to check the model's accuracy and performance at correctly identifying the system memory dump category (Benign, Spyware, Ransomware or Trojan).

To do this the team should test the classifier model on the testing data set previously generated. By testing the accuracy on the unseen testing set the accuracy of the model is obtained. For example, new data having a prediction accuracy of 78%. Small tweaks to the model can improve the accuracy even further.

However, it's important to choose a good evaluation metric that is appropriate to test a machine learning model. Two very popular metrics for testing a Random Forest classifier is a Confusion Matrix and Area Under Curve-Receiver Operating Characteristic (AUC-ROC).

A Confusion Matrix will show the results of how well the model correctly and incorrectly predicted the outcome. Scikit also provide a function to perform this evaluation metric called "confusion_matrix()" giving the team an easy implementation. When loading in the labels it will let the team know how accurate the classifier is performing and with the results of how many wrong predications are being made be able to know where the model is failing and improve the prediction outcome. Run the classifier through the metric again to test for lower incorrect predictions. A simple example can be seen in figure 2 to give the team an idea.

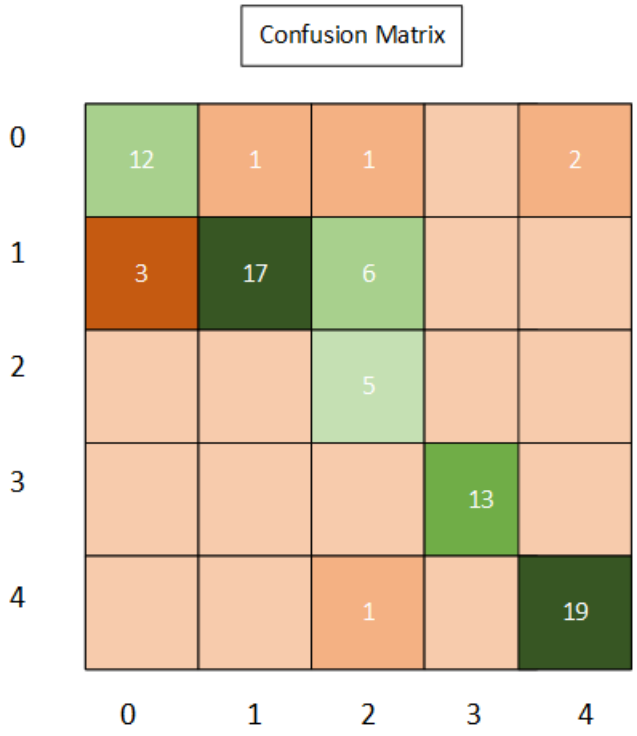

Figure 2: Confusion Matrix example

Another popular evaluation metric is AUC-ROC. Like Confusion Matrix Scikit also provide a function to perform this evaluation metric called "roc_curve()". The closer the AUC is to 1, the better. Area Under the Curve (AUC) of 1.00 is ideal. The classifier can be evaluated on how close it gets to the ideal. A simple example can be seen in figure 3 on the next page to give the team an idea.

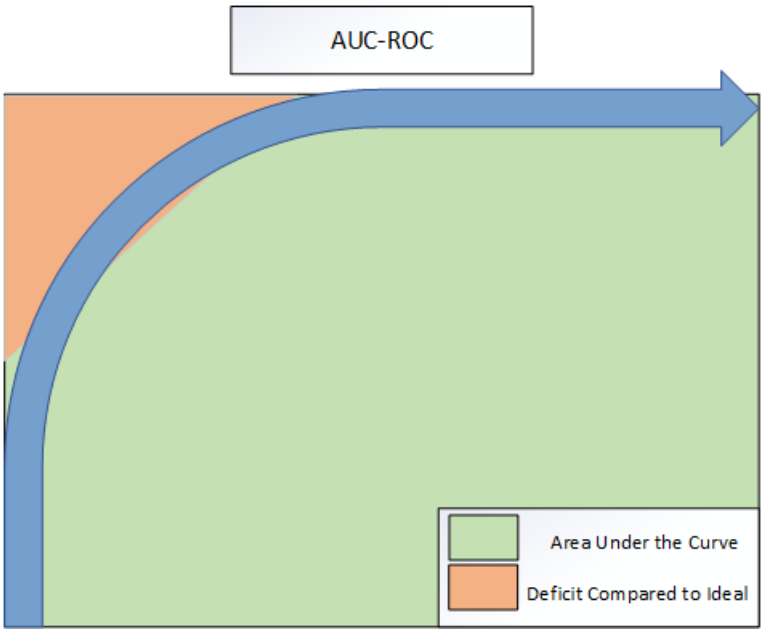

Figure 3: AUC-ROC example

Conclusion

Finally, now that the Random Forest classifier has been built and has been evaluated the final stage is to communicate the results. How effective and accurate is the model's prediction? Does the Random Forest classifier now help the technical team make sense of the memory dump files? Most importantly, is ScottishGlen reasonably safe from the hacktivist threat now that a classification model is in place to rapidly analyse suspicious memory files? If any doubt is at the stage, it may be necessary to redesign the classifier and possibly even choose a new machine learning algorithm (such as Naïve Bayes as discussed) to test its prediction outcomes.

Appendices

Appendix A - Training Dataset

Category	pslist.npro	pslist.nppi	pslist.avg_	pslist.npro	pslist.avg_	dlllist.ndlls	dlllist.avg_	handles.nh	handles.av	handles.np	handles.nf	handles.ne	handles.nd	handles.nk	handles.nt	handles.nd	handles.ns	handles.nt	handles.ns	handles.nr	ldrmodules	ldrmodules	ldrmodules	ldrmodules	ldrmodules	ldrmodules	malfind.nii	malfind.co	malfind.pr	malfind.un	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	modules.n	svcscan.ns	svcscan.ke	svcscan.fs	svcscan.pr	svcscan.sh	svcscan.int	svcscan.na	callbacks.r	callbacks.r	callbacks.r	Class
Benign	45	17	10.55556	0	202.8444	1694	38.5	9129	212.3023	0	670	3161	46	716	887	104	671	125	184	257	53	95	53	0.030372	0.054441	0.030372	5	21	30	1.25	2	0	3	2	7	4	9	0.042553	0	0.06383	0.042553	0.148936	0.085106	0.191489	138	389	221	26	24	116	0	121	87	0	8	Benign
Benign	47	19	11.53191	0	242.234	2074	44.12766	11385	242.234	0	840	3761	51	1011	1030	117	766	148	337	394	77	123	77	0.036167	0.057774	0.036167	12	77	72	1.714286	0	0	0	0	4	2	6	0	0	0	0	0.085106	0.042553	0.12766	138	392	222	26	24	118	0	122	87	0	8	Benign
Benign	40	14	14.725	0	288.225	1932	48.3	11529	288.225	0	1050	3996	45	784	1241	100	645	138	369	338	51	89	51	0.026114	0.045571	0.026114	5	6	30	1.25	0	0	0	0	4	2	5	0	0	0	0	0.1	0.05	0.125	137	395	222	26	27	118	0	120	88	0	8	Benign
Benign	32	13	13.5	0	264.2813	1445	45.15625	8457	264.2813	0	630	2961	36	654	792	83	567	127	186	242	31	62	31	0.021483	0.042966	0.021483	2	2	12	1	0	0	0	0	4	2	6	0	0	0	0	0.125	0.0625	0.1875	138	395	222	26	27	118	0	120	88	0	8	Benign
Benign	42	16	11.45238	0	281.3333	2067	49.21429	11816	281.3333	0	908	3834	45	1252	942	103	825	135	375	429	102	143	102	0.04782	0.067042	0.04782	12	77	72	2	4	0	4	4	8	6	10	0.086957	0	0.086957	0.086957	0.173913	0.130435	0.217391	138	392	222	26	24	118	0	124	87	0	8	Benign
Benign	40	12	13.8	0	306.95	2082	52.05	12278	306.95	0	1080	4308	44	887	1199	101	768	140	381	382	76	113	76	0.036574	0.054379	0.036574	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	43	13	13.81395	0	305.0233	2169	50.44186	13116	305.0233	0	1150	4727	48	923	1314	107	784	145	438	399	70	111	70	0.032833	0.052064	0.032833	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	42	16	11.45238	0	281.4048	2067	49.21429	11819	281.4048	0	908	3835	45	1252	944	103	825	135	375	429	102	143	102	0.04782	0.067042	0.04782	12	77	72	2	4	0	4	4	8	6	10	0.086957	0	0.086957	0.086957	0.173913	0.130435	0.217391	138	392	222	26	24	118	0	124	87	0	8	Benign
Benign	42	16	11.45238	0	281.2619	2067	49.21429	11813	281.2619	0	908	3836	45	1252	945	103	825	135	375	429	102	143	102	0.04782	0.067042	0.04782	12	77	72	2	4	0	4	4	8	6	10	0.086957	0	0.086957	0.086957	0.173913	0.130435	0.217391	138	392	222	26	24	118	0	124	87	0	8	Benign
Benign	40	12	13.875	0	308	2082	52.05	12320	308	0	1080	4321	44	887	1213	101	768	140	384	383	76	113	76	0.036574	0.054379	0.036574	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	43	13	13.37209	0	302.5116	2170	50.46512	13008	302.5116	0	1145	4671	48	910	1264	107	783	145	443	400	70	111	70	0.032818	0.052039	0.032818	5	6	30	1.25	3	0	3	3	7	5	9	0.065217	0	0.065217	0.065217	0.152174	0.108696	0.195652	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	38	13	14.68421	0	290.3947	1875	49.34211	11035	290.3947	0	1027	3789	42	738	1171	96	635	131	355	326	51	87	51	0.026899	0.045886	0.026899	4	5	24	1.333333	2	0	2	2	6	4	7	0.05	0	0.05	0.05	0.15	0.1	0.175	137	395	222	26	27	118	0	120	88	0	8	Benign
Benign	32	13	13.09375	0	264.375	1452	45.375	8460	264.375	0	636	2971	36	658	766	83	571	127	186	242	32	63	32	0.022069	0.043448	0.022069	2	2	12	1	0	0	0	0	4	2	5	0	0	0	0	0.125	0.0625	0.15625	138	395	222	26	27	118	0	119	88	0	8	Benign
Benign	50	22	11.2	0	274.08	2448	48.96	13704	274.08	0	1000	4545	55	1321	1133	120	993	158	441	466	109	158	109	0.043237	0.062674	0.043237	16	81	96	1.777778	1	0	1	1	5	3	7	0.019608	0	0.019608	0.019608	0.098039	0.058824	0.137255	138	393	222	26	25	118	0	127	87	0	8	Benign
Benign	40	12	13.225	0	304.975	2082	52.05	12199	304.975	0	1072	4283	44	887	1164	101	768	140	384	383	76	113	76	0.036574	0.054379	0.036574	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	43	12	13.48837	0	302.2558	2223	51.69767	12997	302.2558	0	1173	4565	47	888	1272	111	776	145	455	445	80	121	80	0.03643	0.0551	0.03643	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	50	22	11.08	0	273.42	2448	48.96	13671	273.42	0	996	4537	55	1320	1125	120	993	158	441	466	109	158	109	0.043237	0.062674	0.043237	16	81	96	1.777778	0	0	0	0	4	2	6	0	0	0	0	0.08	0.04	0.12	138	393	222	26	25	118	0	127	87	0	8	Benign
Benign	40	12	13.325	0	305.475	2082	52.05	12219	305.475	0	1075	4287	44	887	1167	101	768	140	384	383	76	113	76	0.036574	0.054379	0.036574	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	43	12	13.44186	0	301.0233	2223	51.69767	12944	301.0233	0	1153	4572	47	888	1272	111	776	145	440	424	80	121	80	0.03643	0.0551	0.03643	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	50	22	11.04	0	272.32	2448	48.96	13616	272.32	0	987	4520	55	1320	1119	120	993	157	441	466	109	158	109	0.043237	0.062674	0.043237	16	81	96	1.777778	0	0	0	0	4	2	6	0	0	0	0	0.08	0.04	0.12	138	393	222	26	25	118	0	127	87	0	8	Benign
Benign	55	21	11	0	259.6545	2557	46.49091	14283	269.4906	0	1210	4858	58	1168	1267	123	901	159	520	477	106	156	106	0.041536	0.061129	0.041536	12	61	72	1.714286	11	0	13	11	17	13	19	0.166667	0	0.19697	0.166667	0.257576	0.19697	0.287879	138	392	222	26	24	118	0	127	87	0	8	Benign
Benign	41	12	13.39024	0	306.3659	2149	52.41463	12561	306.3659	0	1089	4408	45	930	1209	103	771	143	416	410	87	125	87	0.040353	0.057978	0.040353	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	42	12	13.04762	0	301.0714	2173	51.7381	12645	301.0714	0	1139	4493	46	877	1201	105	770	142	417	396	78	118	78	0.036381	0.055037	0.036381	5	6	30	1.25	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	395	222	26	27	118	0	124	88	0	8	Benign
Ransomwa	32	13	10.375	0	183	1177	36.78125	5856	183	0	557	1845	33	435	530	81	406	92	87	186	36	67	36	0.029703	0.055281	0.029703	2	2	12	1	0	0	0	0	4	2	5	0	0	0	0	0.125	0.0625	0.15625	137	385	220	26	23	114	0	116	88	0	8	Malware
Benign	39	12	12.46154	0	275.5128	1881	48.23077	10746	282.7895	0	910	3743	42	811	1002	96	720	136	313	309	68	102	68	0.036977	0.055465	0.036977	4	5	24	1.333333	4	0	5	4	9	6	11	0.093023	0	0.116279	0.093023	0.209302	0.139535	0.255814	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	41	12	13.5122	0	307.6829	2171	52.95122	12615	307.6829	0	1089	4424	45	930	1218	103	777	143	419	417	89	127	89	0.040826	0.058257	0.040826	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	42	12	13.07143	0	301.2381	2173	51.7381	12652	301.2381	0	1139	4496	46	877	1205	105	770	142	417	396	78	118	78	0.036381	0.055037	0.036381	5	6	30	1.25	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	41	12	13.43902	0	307.439	2133	52.02439	12605	307.439	0	1111	4484	45	901	1196	103	770	141	428	399	75	112	75	0.035868	0.053563	0.035868	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	62	23	10.48387	0	236.3548	2682	43.25806	14660	261.7857	0	1095	4947	62	1239	1370	131	925	174	520	501	107	160	107	0.04003	0.059858	0.04003	16	67	96	1.777778	2	0	8	2	12	4	15	0.03125	0	0.125	0.03125	0.1875	0.0625	0.234375	138	392	222	26	24	118	0	128	87	0	8	Benign
Benign	41	12	13.5122	0	307.8049	2171	52.95122	12620	307.8049	0	1090	4425	45	930	1219	103	777	143	419	417	89	127	89	0.040826	0.058257	0.040826	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	42	12	13.40476	0	305.5238	2195	52.2619	12832	305.5238	0	1150	4577	46	877	1243	105	780	142	428	403	80	120	80	0.0369	0.055351	0.0369	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	52	20	10.94231	0	242.75	2221	43.54902	12623	242.75	0	961	4412	57	1043	1153	123	797	157	395	386	82	130	82	0.037358	0.059226	0.037358	6	7	36	1.2	9	0	9	9	13	11	17	0.147541	0	0.147541	0.147541	0.213115	0.180328	0.278689	138	392	222	26	24	118	0	128	87	0	8	Benign
Benign	39	12	12.38462	0	276.2821	1884	48.30769	10776	283.5789	0	913	3754	42	813	1002	96	720	136	315	311	69	103	69	0.037439	0.055887	0.037439	4	5	24	1.333333	3	0	4	3	8	5	10	0.071429	0	0.095238	0.071429	0.190476	0.119048	0.238095	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	42	12	13.7381	0	308.3095	2195	52.2619	12949	308.3095	0	1159	4628	46	877	1280	105	780	142	437	403	80	120	80	0.0369	0.055351	0.0369	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	40	12	13.85	0	311.2	2060	51.5	12448	311.2	0	1104	4440	44	887	1191	101	759	138	427	391	66	102	66	0.032852	0.050772	0.032852	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	55	20	10.87273	0	245.2727	2385	44.16667	13490	245.2727	0	1059	4822	60	1037	1248	129	817	160	434	403	85	136	85	0.035986	0.057578	0.035986	6	7	36	1.2	5	0	5	5	9	7	15	0.083333	0	0.083333	0.083333	0.15	0.116667	0.25	138	392	222	26	24	118	0	128	87	0	8	Benign
Benign	41	12	13.41463	0	307.1707	2171	52.95122	12594	307.1707	0	1090	4421	45	930	1211	103	777	143	409	417	89	127	89	0.040826	0.058257	0.040826	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	42	12	13.7619	0	308.3095	2195	52.2619	12949	308.3095	0	1159	4629	46	877	1283	105	780	142	439	403	80	120	80	0.0369	0.055351	0.0369	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	53	20	11.41509	0	252.6415	2345	44.24528	13390	252.6415	0	1063	4757	59	1039	1254	127	820	161	433	398	84	134	84	0.036191	0.057734	0.036191	6	7	36	1.2	4	0	4	4	8	6	11	0.070175	0	0.070175	0.070175	0.140351	0.105263	0.192982	138	392	222	26	24	118	0	128	87	0	8	Benign
Benign	41	12	13.85366	0	312.7317	2180	53.17073	12822	312.7317	0	1130	4473	45	932	1242	103	782	143	435	453	89	127	89	0.040658	0.058017	0.040658	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	40	16	10.725	0	253.275	1745	43.625	10132	259.7949	0	798	3519	44	845	816	99	707	127	315	318	73	110	73	0.041336	0.062288	0.041336	3	4	18	1.5	10	0	11	10	15	12	17	0.2	0	0.22	0.2	0.3	0.24	0.34	138	392	222	26	24	118	0	126	87	0	8	Benign
Benign	43	12	12.72093	0	284.5581	2168	50.4186	12236	284.5581	0	1070	4343	47	826	1180	107	759	146	420	377	86	126	86	0.039504	0.057878	0.039504	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	122	88	0	8	Benign
Benign	44	12	12.45455	0	286.9091	2153	48.93182	12624	286.9091	0	1129	4702	48	791	1193	108	750	143	427	347	74	116	74	0.034906	0.054717	0.034906	4	5	24	1.333333	1	0	1	1	5	3	7	0.022222	0	0.022222	0.022222	0.111111	0.066667	0.155556	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	40	12	12.85	0	293.275	1985	49.625	11731	293.275	0	1110	4147	44	803	1107	101	729	141	438	333	64	100	64	0.033126	0.05176	0.033126	3	4	18	1.5	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	43	12	12.60465	0	283.9767	2168	50.4186	12211	283.9767	0	1070	4333	47	826	1165	107	759	146	420	377	86	126	86	0.039504	0.057878	0.039504	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	122	88	0	8	Benign
Benign	44	12	12.45455	0	286.6591	2151	48.88636	12613	286.6591	0	1128	4698	48	791	1190	108	750	143	427	347	74	116	74	0.034939	0.054769	0.034939	4	5	24	1.333333	1	0	1	1	5	3	7	0.022222	0	0.022222	0.022222	0.111111	0.066667	0.155556	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	40	12	12.875	0	293.275	1985	49.625	11731	293.275	0	1110	4146	44	803	1106	101	729	141	438	333	64	100	64	0.033126	0.05176	0.033126	3	4	18	1.5	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	47	17	12	0	264.2766	2147	45.68085	12421	264.2766	0	1056	4409	53	924	1185	114	764	139	422	357	83	128	83	0.038091	0.058743	0.038091	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.085106	0.042553	0.12766	138	392	222	26	24	118	0	126	87	0	8	Benign
Spyware-T	43	17	9.116279	0	194.9535	1576	36.65116	8383	194.9535	0	663	2930	46	720	699	107	607	116	179	255	49	91	49	0.030606	0.056839	0.030606	3	3	18	1	12	0	12	12	16	14	18	0.218182	0	0.218182	0.218182	0.290909	0.254545	0.327273	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	43	17	9.093023	0	194.9535	1577	36.67442	8383	194.9535	0	663	2926	46	720	694	107	607	116	179	255	49	91	49	0.03053	0.056698	0.03053	3	3	18	1	12	0	12	12	16	14	18	0.218182	0	0.218182	0.218182	0.290909	0.254545	0.327273	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	43	17	9.116279	0	194.8372	1576	36.65116	8378	194.8372	0	666	2927	46	720	699	107	607	116	180	256	49	91	49	0.030663	0.056946	0.030663	3	3	18	1	5	0	5	5	9	7	11	0.104167	0	0.104167	0.104167	0.1875	0.145833	0.229167	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	43	17	9.186047	0	194.907	1577	36.67442	8381	194.907	0	665	2921	46	720	699	107	607	116	180	255	49	91	49	0.030625	0.056875	0.030625	3	3	18	1	12	0	12	12	16	14	18	0.218182	0	0.218182	0.218182	0.290909	0.254545	0.327273	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	42	17	9.166667	0	195.2143	1529	36.40476	8199	195.2143	0	657	2888	45	709	677	101	603	113	165	233	47	88	47	0.030401	0.056921	0.030401	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	43	17	9.209302	0	194.8837	1577	36.67442	8380	194.8837	0	665	2929	46	720	703	107	607	116	179	255	49	91	49	0.030663	0.056946	0.030663	3	3	18	1	2	0	2	2	6	4	8	0.044444	0	0.044444	0.044444	0.133333	0.088889	0.177778	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-T	42	16	10.78571	0	210.0714	1623	38.64286	8823	210.0714	0	665	3063	45	679	844	105	652	123	178	261	49	89	49	0.029341	0.053293	0.029341	3	3	18	1	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	389	221	26	24	116	0	122	86	0	8	Malware
Spyware-T	32	13	12.3125	0	192.0625	1168	36.5	6146	192.0625	0	565	1921	33	421	661	81	406	92	86	186	35	66	35	0.029118	0.054908	0.029118	2	2	12	1	2	0	2	2	6	4	7	0.058824	0	0.058824	0.058824	0.176471	0.117647	0.205882	137	385	220	26	23	114	0	115	88	0	8	Malware
Benign	46	17	11.36957	0	254.8913	2021	43.93478	11725	254.8913	0	964	4083	52	926	1072	110	740	136	391	344	79	123	79	0.038555	0.060029	0.038555	4	5	24	1.333333	2	0	2	2	6	4	8	0.041667	0	0.041667	0.041667	0.125	0.083333	0.166667	138	392	222	26	24	118	0	126	87	0	8	Benign
Benign	43	12	12.60465	0	283.9767	2168	50.4186	12211	283.9767	0	1070	4333	47	826	1165	107	759	146	420	377	86	126	86	0.039504	0.057878	0.039504	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	122	88	0	8	Benign
Spyware-T	41	16	10.63415	0	212.8293	1614	39.36585	8726	212.8293	0	651	3054	44	668	812	103	643	126	182	267	47	87	47	0.028313	0.05241	0.028313	3	3	18	1	1	0	1	1	5	3	7	0.02381	0	0.02381	0.02381	0.119048	0.071429	0.166667	138	389	221	26	24	116	0	122	86	0	8	Malware
Benign	40	12	13.325	0	305.3151	2082	52.05	12212	305.3151	0	1073	4287	44	887	1169	101	768	140	384	383	76	113	76	0.036574	0.054379	0.036574	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	44	14	12.6036	0	277.6925	2131	48.43182	12218	277.6925	0	1051	4351	49	833	1172	108	760	153	420	349	70	111	70	0.032957	0.05226	0.032957	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	48	17	11.61105	0	268.2712	2277	47.1006	12971	270.2416	0	1100	4470	54	1015	1183	117	805	146	446	413	90	136	90	0.038871	0.058738	0.038871	5	6	30	1.25	6	0	7	6	11	8	13	0.120809	0	0.127273	0.120809	0.2	0.157173	0.236364	138	392	222	26	24	118	0	126	87	0	8	Benign
Spyware-T	35	14	11.85714	0	191.9143	1262	36.05714	6718	197.5882	0	773	1994	35	452	697	86	456	98	96	208	36	69	36	0.027778	0.053241	0.027778	56	18516	336	14	0	0	1	0	5	2	6	0	0	0.028571	0	0.142857	0.057143	0.171429	137	385	220	26	23	114	0	115	88	0	8	Malware
Spyware-T	44	17	10.13636	0	208.0909	1706	38.77273	9157	212.9535	0	777	3100	46	688	835	108	693	132	190	289	46	88	46	0.026286	0.050286	0.026286	57	18517	342	11.4	0	0	1	0	5	2	7	0	0	0.022727	0	0.113636	0.045455	0.159091	138	389	221	26	24	116	0	122	86	0	8	Malware
Spyware-T	35	14	10.54286	0	186.1714	1273	36.37143	6517	191.6765	0	774	1944	35	455	615	86	462	98	98	208	37	70	37	0.028287	0.053517	0.028287	59	18526	354	14.75	0	0	1	0	5	2	6	0	0	0.028571	0	0.142857	0.057143	0.171429	137	385	220	26	23	114	0	115	88	0	8	Malware
Spyware-T	44	17	9.886364	0	208.7727	1705	38.75	9187	213.6512	0	867	3071	46	693	798	108	696	132	190	289	45	87	45	0.025758	0.0498	0.025758	58	18521	348	11.6	0	0	1	0	5	2	7	0	0	0.022727	0	0.113636	0.045455	0.159091	138	389	221	26	24	116	0	122	86	0	8	Malware
Spyware-T	106	17	3.764151	0	82.58491	1681	15.85849	8818	209.9524	0	920	2985	45	705	727	106	619	122	179	266	47	88	47	0.02845	0.053269	0.02845	9	63	54	2.25	4	0	68	4	72	6	74	0.036364	0	0.618182	0.036364	0.654545	0.054545	0.672727	138	389	221	26	24	116	0	121	87	0	8	Malware
Spyware-T	116	15	3.318966	0	64.52586	1463	12.61207	7564	204.4324	0	915	2466	39	577	655	91	495	105	111	214	41	77	41	0.028792	0.054073	0.028792	8	62	48	2.666667	1	0	80	1	84	3	86	0.008547	0	0.683761	0.008547	0.717949	0.025641	0.735043	138	389	221	26	24	116	0	116	88	0	8	Malware
Spyware-T	122	17	3.245902	0	71.72131	1669	13.68033	8831	215.3902	0	984	2960	44	724	723	104	619	119	179	262	47	87	47	0.029193	0.054037	0.029193	9	63	54	2.25	3	0	84	3	88	5	90	0.024	0	0.672	0.024	0.704	0.04	0.72	138	389	221	26	24	116	0	119	87	0	8	Malware
Benign	41	12	13.43902	0	307.3902	2171	52.95122	12603	307.3902	0	1091	4426	45	930	1214	103	777	143	409	417	89	127	89	0.040826	0.058257	0.040826	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	124	88	0	8	Benign
Trojan-Zeu	41	16	10.17073	0	211.2683	1622	39.56098	8662	211.2683	0	649	3019	44	675	766	103	645	126	181	267	46	86	46	0.027594	0.05159	0.027594	3	3	18	1	1	0	1	1	5	3	7	0.02381	0	0.02381	0.02381	0.119048	0.071429	0.166667	138	389	221	26	24	116	0	123	86	0	8	Malware
Trojan-Zeu	41	16	9.853659	0	208.878	1613	39.34146	8564	208.878	0	649	2989	44	675	728	103	642	126	181	267	45	85	45	0.02719	0.05136	0.02719	3	3	18	1	1	0	1	1	5	3	7	0.02381	0	0.02381	0.02381	0.119048	0.071429	0.166667	138	389	221	26	24	116	0	123	86	0	8	Malware
Trojan-Zeu	40	16	9.875	0	209.1	1564	39.1	8364	209.1	0	646	2920	43	670	704	101	608	123	178	262	45	84	45	0.028107	0.052467	0.028107	3	3	18	1	2	0	2	2	6	4	8	0.047619	0	0.047619	0.047619	0.142857	0.095238	0.190476	138	389	221	26	24	116	0	123	86	0	8	Malware
Trojan-Zeu	39	15	9.974359	0	211.1538	1528	39.17949	8235	211.1538	0	644	2886	42	665	697	100	600	119	177	255	44	83	44	0.028241	0.053273	0.028241	3	3	18	1	3	0	3	3	7	5	9	0.071429	0	0.071429	0.071429	0.166667	0.119048	0.214286	138	389	221	26	24	116	0	122	86	0	8	Malware
Trojan-Zeu	38	15	9.842105	0	210.1842	1453	38.23684	7988	215.8919	0	630	2815	40	673	661	92	596	113	161	230	43	79	43	0.029232	0.053705	0.029232	3	3	18	1	2	0	3	2	7	4	9	0.05	0	0.075	0.05	0.175	0.1	0.225	138	389	221	26	24	116	0	120	86	0	8	Malware
Ransomwa	39	15	9.948718	0	211.1538	1523	39.05128	8235	211.1538	0	638	2891	42	666	696	100	600	119	176	257	44	82	44	0.028351	0.052835	0.028351	3	3	18	1	4	0	4	4	8	6	10	0.093023	0	0.093023	0.093023	0.186047	0.139535	0.232558	138	389	221	26	24	116	0	121	86	0	8	Malware
Trojan-Zeu	39	15	11.4359	0	221.0769	1569	40.23077	8622	221.0769	0	645	3004	42	660	831	99	640	120	177	259	46	84	46	0.028501	0.052045	0.028501	3	3	18	1	3	0	3	3	7	5	9	0.071429	0	0.071429	0.071429	0.166667	0.119048	0.214286	138	389	221	26	24	116	0	123	86	0	8	Malware
Trojan-Zeu	35	14	10.34286	0	215.2	1384	39.54286	7532	215.2	0	627	2627	37	604	633	88	572	107	138	223	43	77	43	0.030561	0.054726	0.030561	2	2	12	1	2	0	2	2	6	4	8	0.054054	0	0.054054	0.054054	0.162162	0.108108	0.216216	138	389	221	26	24	116	0	120	86	0	8	Malware
Ransomwa	45	18	9.333333	0	204.4667	1738	38.62222	9201	204.4667	0	848	3101	48	753	759	111	669	132	192	290	50	94	50	0.028011	0.052661	0.028011	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.088889	0.044444	0.133333	138	389	221	26	24	116	0	122	86	0	8	Malware
Ransomwa	43	16	9.465116	0	203.2326	1655	38.48837	8740	208.0952	0	662	3036	45	692	735	106	651	129	201	273	47	88	47	0.027761	0.051979	0.027761	5	6	30	1.25	0	0	1	0	5	2	7	0	0	0.023256	0	0.116279	0.046512	0.162791	138	389	221	26	24	116	0	123	87	0	8	Malware
Ransomwa	35	14	10.37143	0	215.2857	1379	39.4	7535	215.2857	0	622	2632	37	605	637	88	572	107	138	223	43	77	43	0.03067	0.054922	0.03067	2	2	12	1	0	0	0	0	4	2	6	0	0	0	0	0.114286	0.057143	0.171429	138	389	221	26	24	116	0	119	87	0	8	Malware
Ransomwa	42	16	9.666667	0	204	1616	38.47619	8568	204	0	665	2984	45	683	736	105	645	120	181	263	47	88	47	0.028279	0.052948	0.028279	3	3	18	1	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	389	221	26	24	116	0	122	86	0	8	Malware
Ransomwa	32	13	12.375	0	193.9375	1177	36.78125	6206	193.9375	0	569	1951	33	432	660	81	406	92	88	186	36	67	36	0.029703	0.055281	0.029703	2	2	12	1	0	0	0	0	4	2	5	0	0	0	0	0.125	0.0625	0.15625	137	385	220	26	23	114	0	116	88	0	8	Malware
Benign	42	12	13.26124	0	302.5	2177	51.85681	12705	302.5	0	1140	4510	46	877	1221	105	771	142	421	403	78	118	78	0.036524	0.055133	0.036524	5	6	30	1.25	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	41	12	13.087	0	295.4858	2029	49.4878	12114	295.4858	0	1134	4357	45	805	1167	103	736	142	451	337	65	102	65	0.032878	0.051593	0.032878	3	4	18	1.5	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	40	12	12.95172	0	289.3606	1985	48.87396	11756	293.9162	0	1113	4141	44	803	1134	101	729	141	436	333	64	100	64	0.033126	0.05176	0.033126	3	4	18	1.5	0	0	0	0	4	2	6	0	0	0.015445	0	0.113901	0.049228	0.163129	138	395	222	26	27	118	0	122	88	0	8	Benign
Ransomwa	38	15	9.947368	0	209.5263	1446	38.05263	7963	215.2162	0	629	2815	40	667	664	92	596	113	163	230	43	79	43	0.029533	0.054258	0.029533	3	3	18	1	0	0	1	0	5	2	7	0	0	0.026316	0	0.131579	0.052632	0.184211	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	35	14	10.48571	0	215.8	1385	39.57143	7553	215.8	0	627	2636	37	604	643	88	572	107	137	223	43	77	43	0.03054	0.054688	0.03054	2	2	12	1	0	0	0	0	4	2	6	0	0	0	0	0.114286	0.057143	0.171429	138	389	221	26	24	116	0	120	87	0	8	Malware
Ransomwa	37	15	10.16216	0	215.7568	1447	39.10811	7983	215.7568	0	628	2815	40	674	667	92	596	113	162	230	43	79	43	0.029352	0.053925	0.029352	3	3	18	1	1	0	1	1	5	3	7	0.026316	0	0.026316	0.026316	0.131579	0.078947	0.184211	138	389	221	26	24	116	0	119	87	0	8	Malware
Ransomwa	39	15	10.05128	0	212.4615	1526	39.12821	8286	212.4615	0	639	2904	42	689	704	100	604	119	176	257	44	82	44	0.028278	0.052699	0.028278	3	3	18	1	4	0	4	4	8	6	10	0.093023	0	0.093023	0.093023	0.186047	0.139535	0.232558	138	389	221	26	24	116	0	121	88	0	8	Malware
Ransomwa	45	17	9.533333	0	199.9778	1688	37.51111	9000	204.5455	0	703	3078	47	700	803	109	645	129	220	263	47	90	47	0.027121	0.051933	0.027121	3	3	18	1	1	0	2	1	6	3	8	0.021739	0	0.043478	0.021739	0.130435	0.065217	0.173913	138	389	221	26	24	116	0	122	87	0	8	Malware
Ransomwa	38	16	9.868421	0	211.6316	1473	38.76316	8042	211.6316	0	633	2829	41	681	666	95	604	113	165	231	44	81	44	0.02953	0.054362	0.02953	5	6	30	1.25	4	0	4	4	8	6	10	0.095238	0	0.095238	0.095238	0.190476	0.142857	0.238095	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	43	16	10.60465	0	208.1163	1665	38.72093	8949	208.1163	0	664	3105	46	688	851	107	661	126	181	271	49	91	49	0.028605	0.053123	0.028605	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	389	221	26	24	116	0	122	86	0	8	Malware
Trojan-Zeu	39	15	10.74359	0	217.9231	1558	39.94872	8499	217.9231	0	645	2968	42	660	777	99	634	120	177	259	46	84	46	0.028696	0.052402	0.028696	3	3	18	1	2	0	2	2	6	4	8	0.04878	0	0.04878	0.04878	0.146341	0.097561	0.195122	138	389	221	26	24	116	0	123	86	0	8	Malware
Ransomwa	32	13	10.9375	0	186.3125	1177	36.78125	5962	186.3125	0	558	1886	33	432	578	81	406	92	88	186	36	67	36	0.029703	0.055281	0.029703	2	2	12	1	0	0	0	0	4	2	5	0	0	0	0	0.125	0.0625	0.15625	137	385	220	26	23	114	0	116	88	0	8	Malware
Spyware-1	38	15	10.10526	0	215.3947	1495	39.34211	8185	215.3947	0	638	2874	41	682	689	98	598	116	176	254	45	82	45	0.029625	0.053983	0.029625	3	3	18	1	2	0	2	2	6	4	8	0.05	0	0.05	0.05	0.15	0.1	0.2	138	389	221	26	24	116	0	119	87	0	8	Malware
Ransomwa	39	15	9.948718	0	211.1538	1523	39.05128	8235	211.1538	0	638	2891	42	666	696	100	600	119	176	257	44	82	44	0.028351	0.052835	0.028351	3	3	18	1	4	0	4	4	8	6	10	0.093023	0	0.093023	0.093023	0.186047	0.139535	0.232558	138	389	221	26	24	116	0	121	86	0	8	Malware
Benign	39	12	13.29192	0	302.6765	1995	51.16173	11804	302.6765	0	1046	4154	43	864	1124	99	751	137	367	352	62	98	62	0.031356	0.049562	0.031356	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.102564	0.051282	0.153846	138	395	222	26	27	118	0	123	88	0	8	Benign
Spyware-1	37	15	10.24324	0	215.4324	1446	39.08108	7971	215.4324	0	624	2819	40	673	670	92	594	113	161	230	42	78	42	0.028787	0.053461	0.028787	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	119	87	0	8	Malware
Trojan-Zeu	41	17	9.463415	0	200.7561	1515	37.875	8231	205.775	0	655	2908	43	697	687	98	606	116	169	234	45	84	45	0.029841	0.055703	0.029841	6	18	36	1.5	0	0	0	0	4	2	7	0	0	0	0	0.097561	0.04878	0.170732	138	389	221	26	24	116	0	119	87	0	8	Malware

Appendix B - Testing Dataset

Category	pslist.npro	pslist.nppi	pslist.avg_	pslist.npro	pslist.avg_	dlllist.ndlls	dlllist.avg_	handles.nh	handles.av	handles.np	handles.nf	handles.ne	handles.nc	handles.nk	handles.nt	handles.nc	handles.ns	handles.nt	handles.ns	handles.nr	ldrmodules	ldrmodules	ldrmodules	ldrmodules	ldrmodules	ldrmodules
Benign	71	22	9.71831	0	234.4366	3006	42.33803	16653	264.3333	0	1421	5913	69	1275	1512	143	1011	182	618	517	127	187	127	0.042095	0.061982	0.042095
Benign	41	12	13.60976	0	308	2149	52.41463	12628	308	0	1092	4427	45	930	1231	103	771	143	416	410	87	125	87	0.040353	0.057978	0.040353
Benign	42	12	13.30952	0	302.5	2179	51.88095	12705	302.5	0	1139	4511	46	877	1223	105	770	142	417	402	78	118	78	0.036279	0.054884	0.036279
Benign	70	21	9.628571	0	231.9857	2951	42.15714	16248	266.3607	0	1415	5722	65	1230	1468	139	1001	174	589	512	129	187	129	0.043552	0.063133	0.043552
Spyware-C	37	15	10.18919	0	215.0541	1446	39.08108	7957	215.0541	0	626	2815	40	668	665	92	594	113	162	230	42	78	42	0.028826	0.053535	0.028826
Spyware-C	43	17	9.953488	0	268.4651	1611	37.46512	11545	274.881	0	3537	3026	45	677	794	105	642	120	178	261	48	89	48	0.028968	0.053712	0.028968
Trojan-Sca	38	15	10.05263	0	213.9211	1494	39.31579	8129	213.9211	0	643	2851	41	660	684	98	594	116	177	249	46	83	46	0.030403	0.054858	0.030403
Ransomwa	40	16	9.85	0	208.7	1557	38.925	8348	208.7	0	640	2926	43	664	707	101	608	123	177	262	45	84	45	0.028195	0.052632	0.028195
Ransomwa	43	17	9.27907	0	197.9535	1608	37.39535	8512	197.9535	0	664	2970	46	690	713	107	616	123	178	265	46	88	46	0.027947	0.053463	0.027947
Ransomwa	37	15	10.08108	0	215.6486	1452	39.24324	7979	215.6486	0	635	2813	40	673	659	92	596	113	162	230	43	79	43	0.029332	0.053888	0.029332
Ransomwa	43	17	9.232558	0	195.7442	1582	36.7907	8418	200.4286	0	663	2942	45	684	724	106	608	119	177	259	48	89	48	0.029703	0.055074	0.029703
Trojan-Rec	40	16	9.875	0	208.775	1557	38.925	8351	208.775	0	642	2926	43	665	707	101	606	123	178	262	46	85	46	0.02875	0.053125	0.02875
Benign	42	12	12.96767	0	298.4969	2160	51.42857	12537	305.8017	0	1081	4412	45	922	1192	104	776	144	423	396	80	117	80	0.037754	0.055113	0.037754
Benign	44	12	12.42708	0	264.0559	2052	46.31075	11701	279.3433	0	1019	4122	46	798	1178	103	729	142	364	332	63	102	63	0.031928	0.051256	0.031928
Benign	43	12	12.84022	0	293.2047	2121	49.32558	12607	293.2047	0	1121	4698	47	794	1203	110	745	141	446	357	69	110	69	0.033125	0.052808	0.033125
Benign	40	12	13.33358	0	304.9099	2081	52.02828	12196	304.9099	0	1073	4283	44	887	1163	101	763	140	384	383	76	113	76	0.036589	0.054402	0.036589
Benign	41	14	13.6431	0	297.7107	2064	50.34146	12206	297.7107	0	1091	4222	45	868	1191	102	748	145	426	400	64	103	64	0.031667	0.050965	0.031667
Benign	44	17	11.39523	0	273.998	2131	48.02298	12161	273.998	0	915	4084	48	1138	1013	107	841	142	386	438	100	144	100	0.045742	0.065482	0.045742
Ransomwa	40	16	9.525	0	204.775	1523	38.075	8191	204.775	0	645	2881	43	695	675	98	605	116	161	233	44	83	44	0.02859	0.053931	0.02859
Ransomwa	40	16	9.65	0	205.05	1523	38.075	8202	205.05	0	650	2888	43	695	682	98	605	116	161	233	44	83	44	0.028646	0.054036	0.028646
Ransomwa	40	16	9.65	0	205.05	1523	38.075	8202	205.05	0	650	2888	43	695	682	98	605	116	161	233	44	83	44	0.028646	0.054036	0.028646
Ransomwa	43	16	10.95349	0	211.0233	1677	39	9075	216.0714	0	654	3101	45	683	890	106	698	129	187	280	46	87	46	0.026729	0.050552	0.026729
Benign	43	17	10.40886	0	243.8864	1867	42.46145	10727	249.5837	0	814	3742	48	902	876	106	723	136	343	336	85	126	85	0.04513	0.066684	0.04513
Spyware-C	40	16	10.025	0	214.05	1548	38.7	8563	219.5641	0	850	2895	42	692	722	97	650	119	172	252	43	81	43	0.027546	0.05189	0.027546
Spyware-C	42	16	10.7619	0	208.8571	1618	38.52381	8772	208.8571	0	665	3053	45	678	839	105	648	120	178	262	48	89	48	0.028829	0.053453	0.028829
Trojan-Ref	41	16	9.804878	0	208.2439	1606	39.17073	8538	208.2439	0	645	2985	44	669	724	103	642	126	180	267	46	86	46	0.027896	0.052153	0.027896
Trojan-Ref	40	16	9.85	0	208.625	1557	38.925	8345	208.625	0	642	2921	43	664	704	101	608	123	177	263	46	85	46	0.02884	0.053292	0.02884
Ransomwa	36	14	10.52778	0	182.5833	1313	36.47222	6573	182.5833	0	588	2121	37	488	621	89	464	97	98	191	43	78	43	0.031734	0.057565	0.031734
Ransomwa	37	15	10.24324	0	215.0541	1445	39.05405	7957	215.0541	0	631	2813	40	667	668	92	596	113	160	230	43	79	43	0.029513	0.054221	0.029513
Ransomwa	38	15	9.736842	0	201.9737	1436	37.78947	7675	201.9737	0	643	2676	40	623	640	94	580	107	138	226	45	82	45	0.030801	0.056126	0.030801
Benign	44	12	12.55203	0	286.3614	2153	48.93182	12599	286.3614	0	1133	4660	48	791	1201	108	751	143	439	347	74	116	74	0.034906	0.054717	0.034906
Benign	43	17	10.25955	0	242.3048	1831	41.9804	10573	251.7491	0	807	3696	48	891	858	105	720	133	337	330	84	124	84	0.045089	0.066559	0.045089
Benign	47	18	10.90037	0	246.8121	2144	45.01421	11760	246.8121	0	864	3934	51	1097	984	114	796	150	359	407	83	130	83	0.038174	0.059432	0.038174
Benign	41	12	13.54016	0	307.7107	2149	52.41463	12616	307.7107	0	1091	4432	45	930	1227	103	775	143	416	410	87	125	87	0.040353	0.057978	0.040353
Benign	45	17	10.32252	0	242.5375	1989	44.2	10915	248.0724	0	839	3738	50	899	902	109	748	145	322	370	94	136	94	0.046489	0.06726	0.046489
Benign	43	17	10.39086	0	249.0608	1843	42.86047	10710	255.0146	0	826	3753	48	905	858	105	725	134	358	337	75	115	75	0.040193	0.061629	0.040193
Benign	41	12	13.23046	0	303.3489	2160	52.68298	12437	303.3489	0	1081	4335	45	911	1189	103	770	143	416	413	88	126	88	0.040858	0.058372	0.040858
Spyware-T	43	17	9.372093	0	199.1395	1634	38	8563	199.1395	0	662	2982	46	686	717	107	615	126	178	265	46	88	46	0.027512	0.052632	0.027512
Benign	47	19	11.21238	0	244.608	2106	44.3582	11617	244.608	0	848	3912	50	1063	1006	116	779	149	338	392	79	125	79	0.036947	0.058559	0.036947
Benign	42	12	13.02381	0	298.635	2160	51.42857	12543	305.9432	0	1080	4412	45	922	1195	104	776	144	423	396	80	117	80	0.037562	0.054925	0.037562
Benign	42	12	12.63726	0	279.6919	1987	47.30952	11749	293.7265	0	1120	4116	44	803	1147	101	729	141	433	333	64	100	64	0.033126	0.05176	0.033126
Benign	51	21	11.58491	0	263.3199	2440	46.98067	13677	263.3199	0	1072	4633	58	1165	1227	124	890	160	460	440	95	145	95	0.039005	0.059278	0.039005
Benign	44	12	12.5	0	282.7679	2133	48.47727	12441	282.7679	0	1153	4435	48	828	1195	109	745	151	459	350	72	112	72	0.034601	0.053755	0.034601
Benign	44	12	12.55953	0	286.2846	2153	48.93182	12596	286.2846	0	1127	4663	48	791	1205	108	751	143	426	347	74	116	74	0.034906	0.054717	0.034906
Benign	40	12	13.39432	0	300.7182	2001	50.025	12028	300.7182	0	1084	4427	44	767	1172	100	739	136	412	332	63	101	63	0.032192	0.05161	0.032192
Benign	42	13	12.26598	0	278.0745	2064	49.14286	11679	278.0745	0	1033	4122	46	784	1094	105	742	147	396	343	71	110	71	0.0345	0.05345	0.0345
Benign	32	12	12.34548	0	281.6129	1514	47.31513	9013	300.4538	0	689	3104	33	755	755	82	645	122	219	302	50	78	50	0.034015	0.052396	0.034015
Benign	39	12	13.23748	0	302.9571	1996	51.17949	11815	302.9571	0	1049	4160	43	864	1119	99	751	137	367	352	62	98	62	0.031345	0.049545	0.031345
Benign	44	12	12.63636	0	287.4616	2153	48.93182	12648	287.4616	0	1131	4699	48	791	1220	108	750	143	428	347	74	116	74	0.034906	0.054717	0.034906
Benign	44	13	12.86146	0	296.5087	2225	50.57655	13046	296.5087	0	1148	4681	48	908	1241	109	799	147	442	402	76	118	76	0.035018	0.054151	0.035018
Spyware-1	41	16	9.853659	0	208.8049	1613	39.34146	8561	208.8049	0	651	2991	44	670	725	103	642	126	180	267	46	86	46	0.027778	0.051932	0.027778
Spyware-1	40	16	9.875	0	209.175	1564	39.1	8367	209.175	0	648	2927	43	665	704	101	608	123	177	263	46	85	46	0.028714	0.053059	0.028714
Spyware-1	39	15	10.07692	0	212.3077	1530	39.23077	8280	212.3077	0	645	2901	42	683	701	100	600	119	175	257	45	83	45	0.028828	0.053171	0.028828
Trojan-Zeu	41	16	9.463415	0	202.2683	1546	37.70732	8293	202.2683	0	653	2908	44	698	693	103	606	116	175	254	45	85	45	0.028736	0.054278	0.028736
Ransomwa	39	16	10.12821	0	216.359	1530	39.23077	8439	222.0789	0	651	2955	41	735	706	95	653	116	175	243	50	87	50	0.0323	0.056202	0.0323
Ransomwa	37	15	10.24324	0	215.6757	1452	39.24324	7980	215.6757	0	633	2818	40	673	666	92	596	113	162	230	43	79	43	0.029392	0.053999	0.029392
Ransomwa	44	17	9.272727	0	198.4773	1665	37.84091	8733	198.4773	0	669	3042	47	694	743	109	650	126	182	269	49	92	49	0.028638	0.05377	0.028638
Ransomwa	43	17	9.325581	0	197.3953	1580	36.74419	8451	201.2143	0	663	2949	46	688	720	107	607	122	182	257	53	89	53	0.03802	0.063845	0.03802
Spyware-C	38	15	10.23684	0	215.4737	1496	39.36842	8188	215.4737	0	642	2868	41	682	696	98	598	116	177	254	45	82	45	0.029703	0.054125	0.029703
Spyware-C	37	15	10.24324	0	216.1892	1449	39.16216	7999	216.1892	0	631	2831	40	671	674	92	594	113	161	231	43	79	43	0.029372	0.053962	0.029372
Spyware-C	43	16	10.53488	0	203.7209	1615	37.55814	8761	208.5952	0	660	3052	45	672	840	105	648	120	177	260	48	89	48	0.028898	0.053582	0.028898
Spyware-C	43	17	9.325581	0	198.6512	1595	37.09302	8503	202.4524	0	667	2973	46	717	717	103	611	122	171	242	41	64	41	0.047018	0.073394	0.047018
Spyware-C	42	16	10.19048	0	206.3571	1605	38.21429	8667	206.3571	0	671	3023	45	674	793	105	642	120	178	260	48	89	48	0.029162	0.05407	0.029162
Spyware-C	44	17	9.704545	0	200.1136	1637	37.20455	8762	203.7674	0	662	3063	47	683	777	107	651	126	181	269	72	108	72	0.044693	0.067039	0.044693
Benign	44	17	12.089	0	284.2745	2171	49.04498	12583	284.2745	0	947	4244	48	1176	1073	107	863	145	398	447	102	145	102	0.045548	0.064856	0.045548
Benign	30	11	13.16291	0	284.5589	1455	47.75281	8676	294.2513	0	665	3008	33	688	765	79	636	119	212	274	47	74	47	0.033262	0.052033	0.033262
Ransomwa	40	16	9.85	0	208.875	1563	39.075	8355	208.875	0	648	2923	43	664	703	101	606	123	178	262	45	84	45	0.028125	0.0525	0.028125
Ransomwa	39	15	10.02564	0	210.8974	1528	39.17949	8225	210.8974	0	644	2886	42	659	695	100	598	119	176	258	44	82	44	0.028205	0.052564	0.028205
Benign	43	13	13.37209	0	302.5116	2170	50.46512	13008	302.5116	0	1145	4671	48	910	1264	107	783	145	443	400	70	111	70	0.032818	0.052039	0.032818
Benign	38	13	14.68421	0	290.3947	1875	49.34211	11035	290.3947	0	1027	3789	42	738	1171	96	635	131	355	326	51	87	51	0.026899	0.045886	0.026899
Benign	32	13	13.09375	0	264.375	1452	45.375	8460	264.375	0	636	2971	36	658	766	83	571	127	186	242	32	63	32	0.022069	0.043448	0.022069
Benign	50	22	11.2	0	274.08	2448	48.96	13704	274.08	0	1000	4545	55	1321	1133	120	993	158	441	466	109	158	109	0.043237	0.062674	0.043237
Benign	40	12	13.225	0	304.975	2082	52.05	12199	304.975	0	1072	4283	44	887	1164	101	768	140	384	383	76	113	76	0.036574	0.054379	0.036574
Benign	43	12	13.48837	0	302.2558	2223	51.69767	12997	302.2558	0	1173	4565	47	888	1272	111	776	145	455	445	80	121	80	0.03643	0.0551	0.03643
Spyware-T	42	16	10.54762	0	208.4048	1623	38.64286	8753	208.4048	0	660	3045	45	676	822	105	648	120	176	261	48	89	48	0.028743	0.053293	0.028743
Ransomwa	39	15	9.974359	0	210.1282	1521	39	8195	210.1282	0	634	2881	42	657	694	100	600	119	175	257	44	82	44	0.028351	0.052835	0.028351
Ransomwa	38	15	10.02632	0	213.7368	1492	39.26316	8122	213.7368	0	631	2850	41	676	681	98	600	116	175	252	44	81	44	0.029139	0.053642	0.029139
Ransomwa	37	15	10.10811	0	214.5405	1445	39.05405	7938	214.5405	0	626	2806	40	665	661	92	596	113	160	230	43	79	43	0.029472	0.054147	0.029472
Spyware-G	41	16	10.14634	0	210.6829	1621	39.53659	8638	210.6829	0	650	3012	44	674	760	103	643	126	180	267	46	86	46	0.027611	0.051621	0.027611
Spyware-G	40	16	9.925	0	209.15	1563	39.075	8366	209.15	0	647	2927	43	669	709	101	606	123	177	262	45	84	45	0.028037	0.052336	0.028037

Category	malfind.ni	malfind.co	malfind.pr	malfind.un	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	psxview.nc	modules.n	svcscan.ns	svcscan.ke	svcscan.fs	svcscan.pr	svcscan.sh	svcscan.in	svcscan.na	callbacks.r	callbacks.r	callbacks.r	Class
Benign	14	63	84	1.555556	1	0	9	1	13	3	16	0.013889	0	0.125	0.013889	0.180556	0.041667	0.222222	138	393	222	26	25	118	0	128	87	0	8	Benign
Benign	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	5	6	30	1.25	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	13	62	78	1.625	1	0	10	1	14	3	18	0.014085	0	0.140845	0.014085	0.197183	0.042254	0.253521	138	393	222	26	25	118	0	128	87	0	8	Benign
Spyware-C	3	3	18	1	4	0	4	4	8	6	10	0.097561	0	0.097561	0.097561	0.195122	0.146341	0.243902	138	389	221	26	24	116	0	119	87	0	8	Malware
Spyware-C	3	3	18	1	0	0	1	0	5	2	7	0	0	0.023256	0	0.116279	0.046512	0.162791	138	389	221	26	24	116	0	122	87	0	8	Malware
Trojan-Sca	3	3	18	1	2	0	2	2	6	4	8	0.05	0	0.05	0.05	0.15	0.1	0.2	138	389	221	26	24	116	0	120	86	0	8	Malware
Ransomwa	3	3	18	1	4	0	4	4	8	6	10	0.090909	0	0.090909	0.090909	0.181818	0.136364	0.227273	138	389	221	26	24	116	0	122	86	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	389	221	26	24	116	0	122	87	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	120	87	0	8	Malware
Ransomwa	4	4	24	1	1	0	2	1	6	3	8	0.022727	0	0.045455	0.022727	0.136364	0.068182	0.181818	138	389	221	26	24	116	0	121	86	0	8	Malware
Trojan-Rec	3	3	18	1	5	0	5	5	9	7	11	0.111111	0	0.111111	0.111111	0.2	0.155556	0.244444	138	389	221	26	24	116	0	122	86	0	8	Malware
Benign	5	6	30	1.25	0	0	1	0	5	2	7	0.01229	0	0.035806	0.01229	0.129874	0.059323	0.176908	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	3	4	22	1.385408	1	0	3	1	7	3	9	0.025506	0	0.078761	0.025506	0.166772	0.069511	0.204401	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	3	4	18	1.5	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	5	0	0	0	0	0.097561	0.04878	0.121951	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	12	77	76	1.828597	2	0	2	2	6	4	8	0.055327	0	0.055327	0.055327	0.140433	0.09788	0.178735	138	392	222	26	24	118	0	123	87	0	8	Benign
Ransomwa	4	4	24	1	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	4	4	24	1	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	4	4	24	1	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	47	849	282	9.4	11	0	12	11	16	13	18	0.203704	0	0.222222	0.203704	0.296296	0.240741	0.333333	138	389	221	26	24	116	0	122	86	0	8	Malware
Benign	4	5	29	1.251417	6	0	7	6	11	8	13	0.120903	0	0.14089	0.120903	0.220837	0.160877	0.260811	138	392	222	26	24	118	0	126	87	0	8	Benign
Spyware-C	61	18559	366	12.2	10	0	11	10	15	12	17	0.2	0	0.22	0.2	0.3	0.24	0.34	138	389	221	26	24	116	0	119	86	0	8	Malware
Spyware-C	3	3	18	1	2	0	2	2	6	4	8	0.045455	0	0.045455	0.045455	0.136364	0.090909	0.181818	138	389	221	26	24	116	0	122	87	0	8	Malware
Trojan-Ref	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	389	221	26	24	116	0	122	87	0	8	Malware
Trojan-Ref	3	3	18	1	1	0	1	1	5	3	7	0.02439	0	0.02439	0.02439	0.121951	0.073171	0.170732	138	389	221	26	24	116	0	122	87	0	8	Malware
Ransomwa	15	17	90	5	0	0	0	0	4	2	5	0	0	0	0	0.111111	0.055556	0.138889	138	378	219	26	21	110	0	114	88	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.105263	0.052632	0.157895	138	389	221	26	24	116	0	119	86	0	8	Malware
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	4	5	24	1.333333	7	0	9	7	13	9	15	0.144393	0	0.176471	0.144393	0.254902	0.183609	0.294118	138	392	222	26	24	118	0	127	87	0	8	Benign
Benign	13	78	78	1.625	0	0	0	0	4	2	5	0.014177	0	0.014177	0.014177	0.09692	0.055549	0.117606	138	392	222	26	24	118	0	123	87	0	8	Benign
Benign	6	7	36	1.2	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	6	7	36	1.2	7	0	8	7	12	9	14	0.134615	0	0.153846	0.134615	0.230769	0.173077	0.269231	138	392	222	26	24	118	0	127	87	0	8	Benign
Benign	4	5	24	1.333333	9	0	10	9	14	11	16	0.173077	0	0.192308	0.173077	0.269231	0.211538	0.307692	138	392	222	26	24	118	0	126	87	0	8	Benign
Benign	5	6	35	1.202494	0	0	0	0	4	2	6	0	0	0	0	0.097561	0.04878	0.146341	138	395	222	26	27	118	0	123	88	0	8	Benign
Spyware-T	4	4	24	1	1	0	1	1	5	3	7	0.022727	0	0.022727	0.022727	0.113636	0.068182	0.159091	138	389	221	26	24	116	0	122	86	0	8	Malware
Benign	11	76	71	1.729359	0	0	0	0	4	2	6	0	0	0	0	0.084221	0.042111	0.126332	138	392	222	26	24	118	0	122	87	0	8	Benign
Benign	5	6	30	1.25	0	0	1	0	5	2	7	0.022157	0	0.045439	0.022157	0.138567	0.068721	0.185131	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	3	4	18	1.5	0	0	2	0	6	2	8	0	0	0.047619	0	0.142857	0.047619	0.190476	138	395	222	26	27	118	0	122	88	0	8	Benign
Benign	11	34	68	1.451938	2	0	2	2	6	4	8	0.037072	0	0.037072	0.037072	0.111217	0.074145	0.148289	138	392	222	26	24	118	0	127	87	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	3	4	18	1.5	2	0	2	2	6	4	8	0.047619	0	0.047619	0.047619	0.142857	0.095238	0.190476	138	395	222	26	27	118	0	124	88	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	2	3	16	1.652766	3	0	5	3	9	5	11	0.107768	0	0.163532	0.107768	0.275061	0.163532	0.330826	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.102564	0.051282	0.153846	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	4	5	24	1.333333	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	125	88	0	8	Benign
Benign	5	6	34	1.215072	0	0	0	0	4	2	6	0	0	0	0	0.090909	0.045455	0.136364	138	395	222	26	27	118	0	123	88	0	8	Benign
Spyware-1	3	3	18	1	3	0	3	3	7	5	9	0.068182	0	0.068182	0.068182	0.159091	0.113636	0.204545	138	389	221	26	24	116	0	123	86	0	8	Malware
Spyware-1	3	3	18	1	4	0	4	4	8	6	10	0.090909	0	0.090909	0.090909	0.181818	0.136364	0.227273	138	389	221	26	24	116	0	123	86	0	8	Malware
Spyware-1	3	3	18	1	4	0	4	4	8	6	10	0.093023	0	0.093023	0.093023	0.186047	0.139535	0.232558	138	389	221	26	24	116	0	122	86	0	8	Malware
Trojan-Zeu	4	4	24	1	3	0	3	3	7	5	9	0.068182	0	0.068182	0.068182	0.159091	0.113636	0.204545	138	389	221	26	24	116	0	119	86	0	8	Malware
Ransomwa	4	4	24	1	0	0	1	0	5	2	7	0	0	0.025641	0	0.128205	0.051282	0.179487	138	389	221	26	24	116	0	120	87	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	120	86	0	8	Malware
Ransomwa	4	4	24	1	1	0	1	1	5	3	7	0.022222	0	0.022222	0.022222	0.111111	0.066667	0.155556	138	389	221	26	24	116	0	122	87	0	8	Malware
Ransomwa	2	2	12	1	3	0	3	3	7	5	12	0.065217	0	0.065217	0.065217	0.152174	0.108696	0.26087	138	389	221	26	24	116	0	120	56	0	8	Malware
Spyware-C	3	3	18	1	6	0	6	6	10	8	12	0.136364	0	0.136364	0.136364	0.227273	0.181818	0.272727	138	389	221	26	24	116	0	119	86	0	8	Malware
Spyware-C	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	119	86	0	8	Malware
Spyware-C	3	3	18	1	1	0	2	1	6	3	8	0.022727	0	0.045455	0.022727	0.136364	0.068182	0.181818	138	389	221	26	24	116	0	122	86	0	8	Malware
Spyware-C	2	2	12	1	3	0	3	3	7	5	12	0.065217	0	0.065217	0.065217	0.152174	0.108696	0.26087	138	389	221	26	24	116	0	120	55	0	8	Malware
Spyware-C	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.095238	0.047619	0.142857	138	389	221	26	24	116	0	122	86	0	8	Malware
Spyware-C	3	3	18	1	0	0	0	0	4	2	9	0	0	0	0	0.090909	0.045455	0.204545	138	389	221	26	24	116	0	122	54	0	8	Malware
Benign	13	78	82	1.96119	2	0	2	2	6	4	7	0.046489	0	0.046489	0.046489	0.132623	0.089556	0.169653	138	392	222	26	24	118	0	124	87	0	8	Benign
Benign	2	2	12	1.747828	2	0	3	2	7	4	9	0.08798	0	0.117855	0.08798	0.237356	0.14773	0.289227	138	395	222	26	27	118	0	123	88	0	8	Benign
Ransomwa	3	3	18	1	4	0	4	4	8	6	10	0.090909	0	0.090909	0.090909	0.181818	0.136364	0.227273	138	389	221	26	24	116	0	123	86	0	8	Malware
Ransomwa	3	3	18	1	5	0	5	5	9	7	11	0.113636	0	0.113636	0.113636	0.204545	0.159091	0.25	138	389	221	26	24	116	0	122	86	0	8	Malware
Benign	5	6	30	1.25	3	0	3	3	7	5	9	0.065217	0	0.065217	0.065217	0.152174	0.108696	0.195652	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	4	5	24	1.333333	2	0	2	2	6	4	7	0.05	0	0.05	0.05	0.15	0.1	0.175	137	395	222	26	27	118	0	120	88	0	8	Benign
Benign	2	2	12	1	0	0	0	0	4	2	5	0	0	0	0	0.125	0.0625	0.15625	138	395	222	26	27	118	0	119	88	0	8	Benign
Benign	16	81	96	1.777778	1	0	1	1	5	3	7	0.019608	0	0.019608	0.019608	0.098039	0.058824	0.137255	138	393	222	26	25	118	0	127	87	0	8	Benign
Benign	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.1	0.05	0.15	138	395	222	26	27	118	0	123	88	0	8	Benign
Benign	5	6	30	1.25	0	0	0	0	4	2	6	0	0	0	0	0.093023	0.046512	0.139535	138	395	222	26	27	118	0	123	88	0	8	Benign
Spyware-T	4	14	24	1	1	0	1	1	5	3	7	0.023256	0	0.023256	0.023256	0.116279	0.069767	0.162791	138	389	221	26	24	116	0	122	87	0	8	Malware
Ransomwa	3	3	18	1	4	0	4	4	8	6	10	0.093023	0	0.093023	0.093023	0.186047	0.139535	0.232558	138	389	221	26	24	116	0	120	86	0	8	Malware
Ransomwa	3	3	18	1	4	0	4	4	8	6	10	0.095238	0	0.095238	0.095238	0.190476	0.142857	0.238095	138	389	221	26	24	116	0	118	86	0	8	Malware
Ransomwa	3	3	18	1	0	0	0	0	4	2	6	0	0	0	0	0.108108	0.054054	0.162162	138	389	221	26	24	116	0	118	86	0	8	Malware
Spyware-G	3	3	18	1	1	0	1	1	5	3	7	0.02381	0	0.02381	0.02381	0.119048	0.071429	0.166667	138	389	221	26	24	116	0	123	87	0	8	Malware
Spyware-G	3	3	18	1	2	0	2	2	6	4	8	0.047619	0	0.047619	0.047619	0.142857	0.095238	0.190476	138	389	221	26	24	116	0	123	87	0	8	Malware

References

Carrier, T.; Victor, P.; Tekeoglu, A. and Lashkari, A. (2022). Detecting Obfuscated Malware using Memory Feature Engineering. In Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP, ISBN 978-989-758-553-1; ISSN 2184-4356, pages 177-188. DOI: https://doi.org/10.5220/0010908200003120

H. Lashkari, B. Li, T. L. Carrier and G. Kaur, "VolMemLyzer: Volatile Memory Analyzer for Malware Classification using Feature Engineering," 2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS), Hamilton, ON, Canada, 2021, pp. 1-8, doi: https://doi.org/10.1109/RDAAPS48126.2021.9452028

IBM, 2023, What is naïve Bayes, IBM. Available at: https://www.ibm.com/topics/naive-bayes [Accessed: April 16, 2023].

IBM, 2023, What is Random Forest?, IBM. Available at: https://www.ibm.com/topics/random-forest [Accessed: April 16, 2023].

Orza, P, 2022, Document classification: A complete guide, Document Classification: A Complete Guide. Available at: https://levity.ai/blog/document-classification-guide [Accessed: April 23, 2023].

Scikit, 2023, Oob errors for random forests, OOB Errors for Random Forests. Available at: https://scikit-learn.org/stable/auto_examples/ensemble/plot_ensemble_oob.html#sphx-glr-auto-examples-ensemble-plot-ensemble-oob-py [Accessed: April 23, 2023].

Vadapalli, P, 2022, Naive Bayes explained: Function, Advantages & disadvantages, applications in 2023, upGrad blog. Available at: https://www.upgrad.com/blog/naive-bayes-explained/ [Accessed: April 17, 2023].