Unit 2 Case Study

MSDS Fall ‘19

7333 Quantify the World

Daniel Serna, Bruce Granger, and Brandon de la Houssaye

October 8, 2019

**Abstract**

In this paper we provide an in-depth analysis of a machine learning (ML) method that programmatically identifying the difference between emails that are unwanted (spam) from email that are wanted (ham). We will touch upon the history of unwanted emails, the financial impact of malicious spam emails, and who is at risk to spam.

**1 Introduction**

In today’s email reality, people subscribe to email newsletters, forums, alerts, etc. as a means of having information pushed to them automatically. What began as a helpful feature for users slowly turned into a marketing bonanza, as a new form of target marketing. The marketing firms then began to resell email address as they learned more about the users, thus creating value to retailers. Not to be left out of the bonanza, criminals (cyber-criminals) use email as means of attacking new targets through what is known as “phishing” expeditions. The basic aim of a phishing attack is to convince the email receiver to click on an active link that is embedded within the email, which then leads the victim to a fake website that closely resembles a legitimate company and where the user is asked to provide username and password and or other information. The phishing game is very easy for scammers (criminals) to replicate over and over and as a result is one of the easiest forms of cyber-attack for a cyber-criminal to carry out[[1]](#footnote-1). The latest form of attack often begins from email is called “ransomware”. The majority of ransomware is spread via gigantic spam email campaigns that involving hundreds of thousands of emails that are sent daily. In ransomware attack, the receiver is again prompted to click on embedded URLs within the email. Once a user clicks the link, malicious code is downloaded to the user’s machine that encrypts the users hard drive. Once encrypted, the cyber-criminal will lock out the user, then demand a ransom be paid, typically through bitcoin, before the cyber-criminal will unlock the user’s data. Often times malware will pose as ransomware and when victims pay the ransom to the cyber-criminal, the victims’ data is never “unlocked” by the cyber-criminal, this is known as “wiper” malware[[2]](#footnote-2). These attacks do not typically target an individual or organization, they are attacks of opportunity through the economies of scale[[3]](#footnote-3). A report from Cybersecurity Ventures estimated that damages from ransomware attacks cost as much as $8 billion globally in 2018[[4]](#footnote-4). One agent to combat this phenomenon is to make users aware of the dangers of spam email and educate users what to look for and what not to do. Another response to this is to phenomenon is to invest in technologies that stop spam email from ever entering the users “in box”, such as implementing machine learning to route spam to the spam folder and the good email to the inbox, which is the point of this exercise. Given what is at stake, the machine learning algorithm should error on the side of caution and false positives, which means we want to focus on “precision” as measurement to model effectiveness. Worst case, the user can check the emails in their spam folder for an email they are expected, in which case is “ham” email.

**2 Data**

The email message that will be at the core of this analysis is made available SpamAssassin (<http://spamassassin.apache.org>) and for repeatability and convenience these email examples have been bundled into the RSpamData package in the R programming language. The emails have been organized into five (5) subdirectories, three of which identify the good emails (ham) and two identify the unwanted emails (spam). The names of the spam folders are:

* spam
* spam\_2

The names of the ham folders are:

* easy\_ham
* easy\_ham\_2
* hard\_ham

There are a total of nine-thousand three-hundred and fifty-three (9,353) emails and the distribution of spam to ham is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Folder Name | Email Type | Email Count | Type Total | Type % of Total |
| spam | Spam | 1,001 | 2,399 | 25% |
| spam\_2 | Spam | 1,398 |
| easy\_ham | Ham | 5,052 | 6,954 | 75% |
| easy\_ham\_2 | Ham | 1,401 |
| hard\_ham | Ham | 501 |

An email message has two parts, the email header and email body, which mirrors the concept of a standard letter that is sent through the United States Postage system. The email header is similar to the envelope that encapsulates the letter and contains metadata about where the email is going, additional recipients that will also receive the email, routing information. This information is contained in a key: value pair. The body of the email message is analogous to the letter being sent within the postal envelope. The body of the email message is separated from the email header by a single empty line. When an email attachment is added to the email message, the attachment is included in the body of the email message[[5]](#footnote-5). Within the metadata, the Content-Type key communicates if the message has an attachment or not. If the message does not have an attachment, with the value of “TEXT/PLAIN” is provided. If the message has an attachment, the value of “multipart”. In the case where there is an attachment, there is a boundary string. After the initial “boundary” is provided, subsequent boundary string is preceded by two hyphens, except the final boundary where it is preceded and followed by two hyphens.

**3 Data Cleansing**

**4 Methods**

The team ran additional analysis on the spam data by utilizing 5-fold cross validation techniques in an effort to improve our prediction. Both the Naïve-Bayes and Regression Partitioning methods were used for this cross-validation analysis.

**5 Results**

Question 19) Consider the other parameters that can be used to control the recursive partitioning process. Read the documentation for them in the *rpart.control()* documentation.

**Documentation for rpart.control() was provided in:**

<https://www.rdocumentation.org/packages/rpart/versions/4.1-15/topics/rpart.control>

**Also, carry out an Internet search for more information on how to tweak the *rpart()* tuning parameters. Experiment with values for these parameters.**

<https://www.gormanalysis.com/blog/decision-trees-in-r-using-rpart/>

<https://csantill.github.io/RTuningModelParameters/>

<https://www.mayo.edu/research/documents/rpartminipdf/doc-10027257>

**Do the trees that result make sense with your understanding of how the parameters are used?**

Yes, but only to a certain extent. The complexity parameter (cp) seemed to be the most relevant parameter to adjust in setting the output.

**Can you improve the prediction using them?**

Not necessarily (see below). This was the interesting piece. We changed parameters to account for the sample size, the seed, the maximum depth (i.e., number of possible layers in the tree before splitting stops), cross-validations, minimum size of a bucket (observations in any final leaf), minimum split (the minimum number of splits attempted), a complexity parameter (cp). This parameter (cp) can be a set parameter and is also a model output (as can be seen in the original example). By setting a given cp, we dictate the splitting to continue (or stop) if the relative fit is decreased. That is, the model will stop if performing additional splits does not increase the fit.

We have observed that the cp is clearly the most relevant parameter. We could not set the other parameters to improve upon the fit (as measured by cp). In setting a cp to equal the original model (relatively), we did not find any additional ‘leafs’. Or, put another way, we cannot get to more insight/depth of the data if we are aiming to maintain the fit as measured by cp. i.e., the model would not be able improve with any additional splits.

The first set of parameters tuned were the seed; setting na.action to na.rpart; and decreasing the floor (of the sample set to \*/8). We then increased the sample size, set the min\_split to 10, set the max depth to 30, and x-validations to 80. We then set a minimum number of observations to 2, and set a complexity parameter to 0.012.

The tree results are a follows:

**Please input tree results from workbook.**

**The code is provided in appendix X.**

The team’s Naïve-Bayes cross validation analysis allowed us to conclude that utilizing a laplace value of 0 along with usekernel and adjust parameters set to FALSE produced the optimal model. This was determined by the F1 score as see in Figure 4. With this particular model, the team achieved a type I error rate of 0.0463 and type II error rate of 0.0634

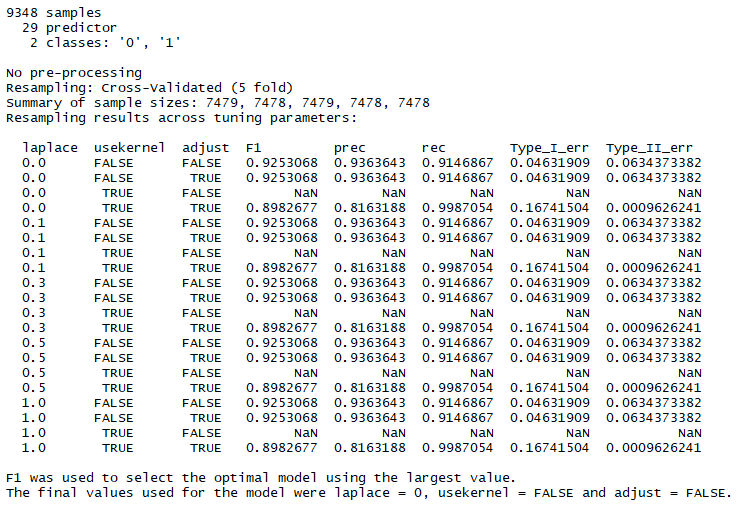


Figure - Naive Bayes CV

The team’s Regression Partition cross validation analysis resulted in an optimal model when a complexity parameter of 0.001 was used. The optimal model was chosen by F1 score as seen in Figure 4. With this model, the team achieved a type I error rate of 0.03 and a type II error rate of 0.026.

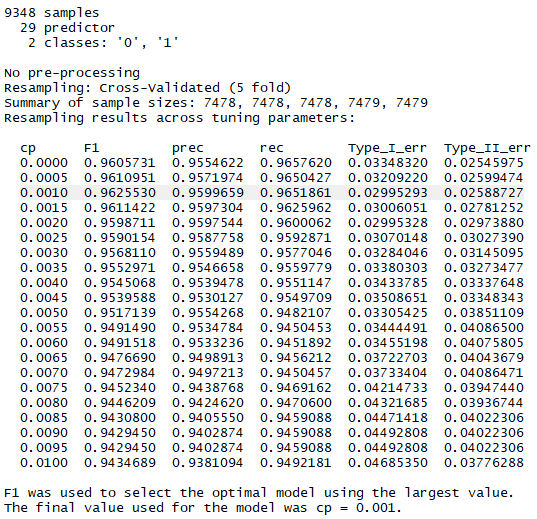


Figure - Regression Partition CV

**6 Conclusion**

The team had difficulty applying the results from cross validation methods to the original data set. We desired to determine a tau threshold value that we could apply to our original analysis to improve prediction. Ultimately, we chose to go a different route and identify optimal parameters for both Naïve-Bayes and Regression Partition models. Future work is warranted to expand on this analysis.

**A Code**

1. https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#4807db156cd3 [↑](#footnote-ref-1)
2. Ibid [↑](#footnote-ref-2)
3. Ibid [↑](#footnote-ref-3)
4. https://www.newsweek.com/texas-ransomware-bitcoin-hackers-1454865 [↑](#footnote-ref-4)
5. Data Science in R, A Case Studies Approach to Computational Reasoning and Problem Solving Deborah Nolan, Duncan Temple Lang page 107 [↑](#footnote-ref-5)