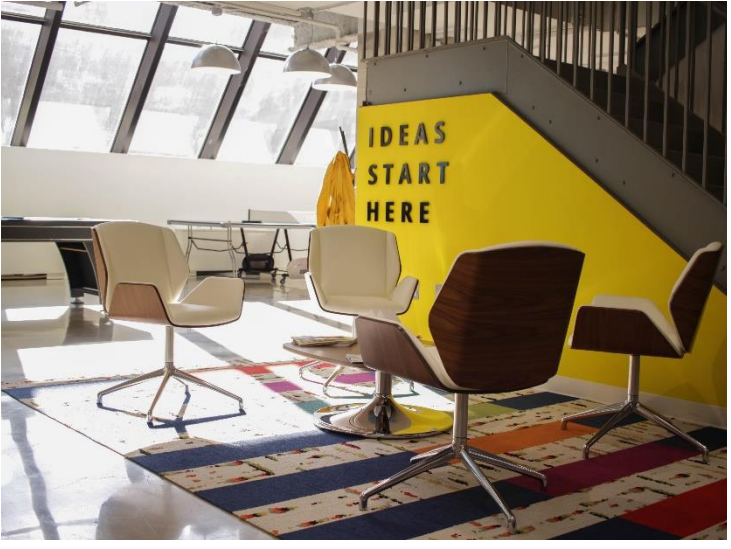


WE SPECIALIZE IN PREDICTING SYSTEMS GOING TO BE INFECTED BY MALWARES

Innovation Geek

MALWARES

- Malwares come in different forms and cause different impacts
  - Choke systems/resources
  - Steal data
  - Encrypted data until “ransom” is paid
- Anti-malwares, firewalls & AVs are reactive approaches and might not be helpful in providing a proactive protective layer as new malwares are discovered at astonishing rate.
  - 70% increase in malwares each year, 795 new malwares every hour i-e 13 new malwares to protect from each min
- Worldwide Impact:
  - 2015: $500 Billion
  - 2019: $2 Trillion
  - 2021: $6 Trillion (Projected)
- How to save your organization from malwares proactively to avoid business loss?

BUILDING PREDICTIVE MACHINE LEARNING MODEL

Data Science has improved our ability to detect threats, Predictive model can help us know the potential malware before it happens.

Data Description:

The data includes computer configuration, owner information, installed software, and configuration information.

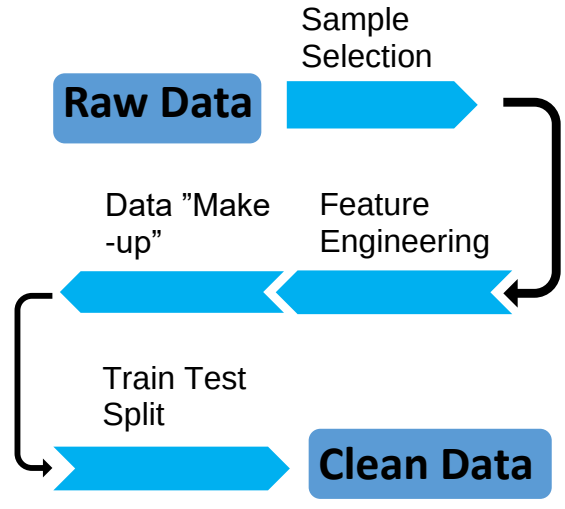
8.9M records

83 features

Some of the important features are

- Operating system
- AV configurations
- AV product installed
- Firmware versions
- Timely Updates
- Platforms

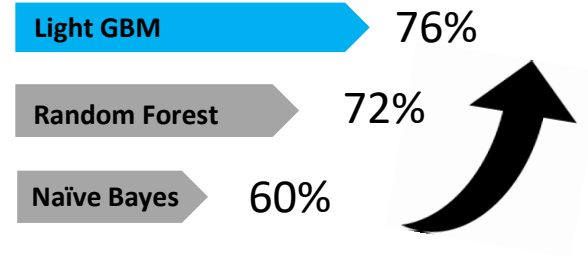
DATA PROCESS PIPELINE



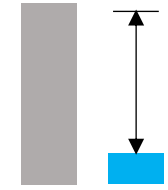
MODEL SELECTION

We used a combined score weighted 55 on recall and 45 on precision as the metric to measure model performance

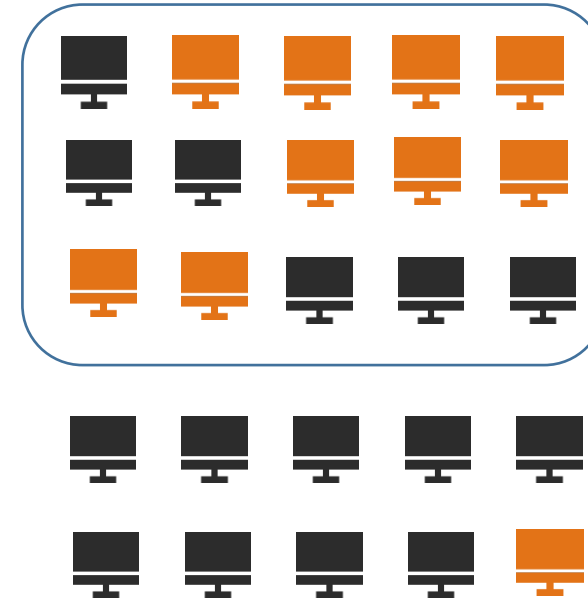
It turns out that the LightGBM classifier is the optimum one by obtaining a combined score of 76 and AUC score of 70%.



MODEL RESULT



Reduce Malware Infection rate by 90% percent



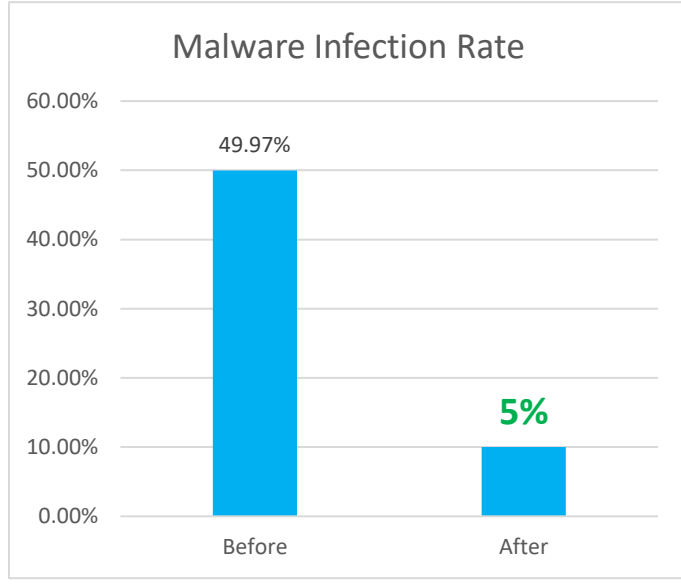
Using the optimal cut off value of 0.24, our model achieves a recall of 90% and precision of 60%.

Our model will detect systems prone to malwares with 90% accuracy, and if proper actions were taken, it will help you to reduce the potential malware attacks by up to **90%**.

ADDING VALUE TO YOUR BUSINESS – COST SAVING

Model Implementation:

- The malware detection rate could reach to 49.97% if clients randomly select machines and software.
- After running our model and taking actions on that, the malware infection rate can sharply decrease to 5 percent, which means that we can help achieve up to 90% detection rate.
- By adjusting our model setting, we can even assure up to 97% safe on your core servers or machines.
- In another words, our model will help you save **180,000** dollars on average from data breach or system crash per year.



FINDING ABOUT ANTIVIRUS SOFTWARE

Our analysis shows that computers with at least one antivirus software do not have a lower malware infection rate. On the contrary, the number of protected computers with malware detections is slightly higher than the ones without protection.

It is hard to tell whether the antivirus software is helpful or not against new malwares. However, its prudent to take all necessary measures.

Our model helps you achieve that level of surety.

OUR RECOMMENDATIONS

There are a few things you need to know to better prepare for the threats of malware.

- ✔ Antivirus software focus mainly on dealing with traditional or more established threats like trojan and worms, but they may fail to detect the latest and currently widespread malwares.
- ✔ Most computer users tend to ignore the routine updates of antivirus software, which further weaken the power of it.
- ✔ All viruses are malware, but not all malware are viruses. Antivirus software don't work efficiently as most people think they do.

Our recommendation is using our model in combination with anti-malwares, firewalls and latest anti viruses to get the maximum benefit.